Summit WM Series WLAN Switch and Altitude Access Point Software Version 4.1 User Guide

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
(408) 579-2800
http://www.extremenetworks.com

Part number: 120386-00 Rev 01

Alpine, Alpine 3804, Alpine 3802, Altitude, BlackDiamond, BlackDiamond 6808, BlackDiamond 6816, EPICenter, Ethernet Everywhere, Extreme Ethernet Everywhere, Extreme Networks, Extreme Turbodrive, Extreme Velocity, ExtremeWare, ExtremeWorks, ExtremeXOS, GlobalPx Content Director, the Go Purple Extreme Solution Partners Logo, Sentriant, ServiceWatch, Summit, Summit24, Summit48, Summit1i, Summit4, Summit5i, Summit7i, Summit 48i, SummitRPS, SummitGbX, Triumph, vMAN, the Extreme Networks logo, the Alpine logo, the BlackDiamond logo, the Summit logos, the Extreme Turbodrive logo, and the Color Purple, among others, are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and other countries. Other names and marks may be the property of their respective owners.

© 2007 Extreme Networks, Inc. All Rights Reserved.

Specifications are subject to change without notice.

Merit is a registered trademark of Merit Network, Inc. Solaris and Java are trademarks of Sun Microsystems, Inc. in the U.S. and other countries. Avaya is a trademark of Avaya, Inc.

All other registered trademarks, trademarks and service marks are property of their respective owners.

The following information is only included in the ExtremeXOS Command Reference Guide:

The ExtremeXOS operating system is based, in part, on the Linux operating system. The machine-readable copy of the corresponding source code is available for the cost of distribution. Please direct requests to Extreme Networks for more information at the following address:

Legal Department
3585 Monroe Street
Santa Clara CA 95051

Contents

About this Guide 9

Who should use this guide 9
What is in this guide 9
Formatting conventions...10
Documentation feedback 10
Safety Information 11
Considerations Before Installing...11
Installing Power Supply Units...12
Power Input Requirements 12
Maintenance Safety..13
General Safety Precautions 13
Power Supply Cords Selection 13
Battery Replacement and Disposal...15
Sicherheitshinweise..16
Hinweise zur Installation...16
Installation von Netzteilen...17
Wartungssicherheit...17
Allgemeine Sicherheitsvorkehrungen 18
Auswahl der Stromkabel 18
Austauschen und Entsorgen von Batterien 19

Chapter 1: Overview of the Summit WM series switch, access points, and WLAN switch software solution21

Conventional wireless LANs..21
Elements of the Summit WM series switch, access points, and WLAN switch software solution.........22
Summit WM series switch, access points, and WLAN switch software and your network 24
Network traffic flow 25
Network security 26
WM Access Domain Services..28
Static routing and routing protocols 28
Packet filtering policy...28
Mobility and roaming..29
Network availability 29
Quality of Service (QoS)..30
System Configuration Overview...30

Chapter 2: Configuring the Summit WM series switch.. 33

System configuration overview...34
Performing the first-time setup of the Summit WM series switch 36
Accessing the Summit WM series switch 36
Connecting the Summit WM series switch to your enterprise network 41
Applying the product license key 41
Setting up the data ports 42
Setting up static routes...45

Setting up OSPF Routing 47
Filtering at the interface level 50
Built-in port-based exception filters 50
User defined port-based exception filters 51
Completing the system configuration 53
Ongoing Operations of the Summit WM series switch, access points, and WLAN switch software 53

Chapter 3: Configuring the Altitude AP 55

Altitude AP overview 55
Discovery and registration overview 56
Altitude AP discovery 57
Registration after discovery 58
Understanding the Altitude AP LED status 58
Configuring the Altitude APs for the first time 60
Defining properties for the discovery process 60
Connecting the Altitude AP to a power source and initiating the discovery and registration process 63
Adding and registering an Altitude AP manually 63
Modifying Altitude AP settings 64
Modifying an Altitude AP’s status 64
Configuring the default AP settings 66
Modifying an Altitude AP’s properties 68
Modifying the Altitude AP’s radio properties 70
Setting up the Altitude AP using static configuration 75
Configuring Dynamic Radio Management 77
Modifying an Altitude AP’s properties based on a default AP configuration 79
Modifying the Altitude AP’s default setting using the Copy to Defaults feature 79
Configuring APs simultaneously 80
Performing Altitude AP software maintenance 81

Chapter 4: WM Access Domain Services (WM-AD) 85

WM-AD overview 85
Setting up a WM-AD checklist 86
Topology of a WM-AD 87
RF assignment for a WM-AD 88
Authentication for a WM-AD 89
Authentication with SSID network assignment 89
Authentication with AAA (802.1x) network assignment 89
Filtering for a WM-AD 90
Final filter rule 91
Filtering sequence 91
WM-AD global settings 92
Setting up a new WM-AD 96

Chapter 5: WM Access Domain Services configuration 97

Topology for a WM-AD 98
Configuring topology for a WM-AD for Captive Portal 98
Configuring topology for a WM-AD for AAA 105
Saving your topology properties 106

Assigning Altitude AP radios to a WM-AD 106
Authentication for a WM-AD 108
Vendor Specific Attributes 108
Defining authentication for a WM-AD for Captive Portal 109
Defining authentication for a WM-AD for AAA 116
Defining MAC-based authentication for a WM-AD 119
Defining accounting methods for a WM-AD 121
Defining RADIUS filter policy for WM-ADs and WM-AD groups 122
Configuring filtering rules for a WM-AD 123
Filtering rules for an exception filter 124
Defining non-authenticated filters 126
Filtering rules for a filter ID group 129
Filtering rules for a default filter 131
Enabling multicast for a WM-AD 133
Configuring privacy for a WM-AD 135
Privacy for a WM-AD for Captive Portal 135
Privacy for a WM-AD for AAA 138
Defining a WM-AD with no authentication 142
Defining priority level and service class for WM-AD traffic 142
Defining the service class for the WM-AD 143
Configuring the priority override 144
Working with Quality of Service (QoS) 144
QoS modes 144
Configuring the QoS policy on a WM-AD 146
Bridging traffic locally 149

Chapter 6: Availability, mobility, and controller functionality 153

Availability overview 153
Availability prerequisites 154
Viewing the Altitude AP availability display 156
Viewing SLP activity 156
Events and actions during a failover 158
Mobility manager 159
Displays for the mobility manager 163
Defining management users 163
Configuring network time 165
Configuring Check Point event logging 167
ELA Management Station events 169
Enabling SNMP 169
MIB support 169
Enabling SNMP on the Summit WM series switch 170
Using controller utilities 171
Configuring Web session timeouts 172

Chapter 7: Working with third-party APs 175

Chapter 8: Working with the Summit WM Series Spy 179

Summit spy overview 179
Enabling the Analysis and data collector engines 180
Running Summit Spy scans 181
Analysis engine overview 183
Working with Summit spy scan results 184
Working with friendly APs 186
Viewing the Summit spy list of third-party APs 188
Maintaining the Summit spy list of APs 189
Viewing the Scanner Status report 190

Chapter 9: Working with reports and displays 191

Viewing the displays 191
Viewing the Altitude AP availability display 193
Viewing statistics for Altitude APs 193
Viewing displays for the mobility manager 196
Viewing reports 198

Chapter 10: Performing system maintenance 203

Performing Altitude AP client management 203
Disassociating a client 203
Blacklisting a client 204
Resetting the AP to its factory default settings 207
Performing system maintenance tasks 208
Performing Summit WM series switch software maintenance 210
Updating Summit WM series switch software 211
Updating operating system software 212
Backing up Summit WM series switch software 214
Restoring Summit WM series switch software 217
Upgrading a Summit WM series switch using SFTP 219
Configuring Summit WM series switch, access points, and WLAN switch software logs and traces 220
Viewing log, alarm and trace messages 220

Glossary 227

Networking terms and abbreviations 227
Summit WM series switch, access points, and WLAN switch software terms and abbreviations 245

Appendix A: System states and LEDs 247

Summit WM series switch system states and LEDs 247
Activity and traffic monitoring 247
Altitude AP system states 248

Appendix B: Regulatory Information 251

Summit WM200 (15955), Summit WM2000 (15956) 251

Safety Standards 251

EMI/EMC Standards 252

Telecom Standards 252

Physical and Environmental 253

Environmental Operating Conditions for Summit WM100/1000, Summit WM200/2000, and Altitude 350-2 AP 253

Altitude 350-2i Integrated Antenna AP (15938), Altitude 350-2d Detachable Antenna AP (15939) 254

United States - FCC Declaration of Conformity Statement 254

Conditions Under Which a Second party may replace a Part 15 Unlicensed Antenna 255

European Community 257

Certifications of Other Countries 263

Index 265

About this Guide

This guide describes how to install, configure, and manage the Summit® WM series switch, access points, and WLAN switch software. This guide is also available as an online help system.

To access the online help system:

1. In the Summit Wireless Assistant Main Menu bar, click **Help**. The About Summit Wireless Assistant screen appears.
2. In the left pane, click **Controller Documentation**. The online help system is launched.

Who should use this guide

This guide is a reference for system administrators who install and manage the Summit WM series switch, access points, and WLAN switch software system.

Any administrator performing tasks described in this guide must have an account with full administrative privileges.

What is in this guide

This guide contains the following:

- About this Guide describes the target audience and content of the guide, the formatting conventions used in it, and how to provide feedback on the guide.
- Chapter 1 provides an overview of the product, its features and functionality.
- Chapter 2 describes how to perform the installation, first-time setup and configuration of the Summit WM series switch, as well as configuring the data ports and defining routing.
- Chapter 3 describes how to install the Altitude AP, how it discovers and registers with the Summit WM series switch, how to view and modify the radio configuration, and how to enable Dynamic Radio Management.
- Chapter 4 provides an overview of WM Access Domain Services (WM-AD), the mechanism by which the Summit WM series switch, access points, and WLAN switch software controls and manages network access.
- Chapter 5 provides detailed instructions in how to configure a WM-AD, its topology, authentication, accounting, RADIUS policy, multicast, filtering and privacy. Both Captive Portal and AAA types of WM-AD are described.
- Chapter 6 describes how to set up the features that provide availability in the event of a controller failover, and mobility for a wireless device user.
- Chapter 7 describes how to use the Summit WM series switch, access points, and WLAN switch software features with third-party wireless APs.
- Chapter 8 explains the security tool that scans for, detects and reports on rogue APs.

- Chapter 9 describes the various reports and displays available in the Summit WM series switch, access points, and WLAN switch software system.
- Chapter 10 describes maintenance activities, such as software upgrades on both the Summit WM series switch and the Altitude AP. This chapter also includes information on the logs, traces, reports and displays available.
- Glossary contains a list of terms and definitions for the Summit WM series switch and the Altitude AP as well as standard industry terms used in this guide.
- Appendix A provides a reference on the LED displays and their significance.
- Appendix B provides the regulatory information for the Summit series switches and the Altitude 350-2 wireless access points (APs).

Formatting conventions

The Summit WM series switch, access points, and WLAN switch software documentation uses the following formatting conventions to make it easier to find information and follow procedures:

- **Bold** text is used to identify components of the management interface, such as menu items and section of pages, as well as the names of buttons and text boxes.
- For example: Click **Logout**.
- `Monospace` font is used in code examples and to indicate text that you type.
- For example: Type `https://<wm100-address>[:mgmt-port>]`
- The following symbols are used to draw your attention to additional information:

NOTE

Notes identify useful information that is not essential, such as reminders, tips, or other ways to perform a task.

WARNING!

Warnings identify information that is essential. Ignoring a warning can adversely affect the operation of your equipment or software.

Documentation feedback

If you have any problems using this document, please contact your next level of support:

- Customers should contact the Extreme Networks Technical Assistance Center (TAC).

When you call, please have the following information ready. This will help us to identify the document that you are referring to.

- Title: Summit WM Series WLAN Switch and Altitude Access Point Software Version 4.1 User Guide
- Part Number: 120369-00

Safety Information

WARNING!

Read the following safety information thoroughly before installing Extreme Networks products. Failure to follow this safety information can lead to personal injury or damage to the equipment.

Installation, maintenance, and removal of a switch, chassis, or any of its components must be performed by trained and qualified service personnel only! Trained and qualified service personnel are persons having appropriate technical training and experience necessary to be aware of the hazards to which they are exposed in performing a task and of measures to minimize the danger to themselves and/or other persons.

Considerations Before Installing

WARNING!

Consider the following items before installing equipment.

Ensure that the following conditions are met:

- The system is designed to operate in a typical Telco environmental controlled environment. Choose a site that has the following characteristics:
  - Temperature and humidity controlled indoor area where maximum ambient room temperature shall not exceed 40ºC (104ºF)
  - Clean and free from airborne materials that can conduct electricity.
  - Well-ventilated and away from sources of heat including direct sunlight.
  - Away from sources of vibration or physical shock.
  - Isolated from strong electromagnetic fields produced by electrical devices.
  - Secured, enclosed, and restricted access, ensuring that only trained and qualified service personnel have access to the equipment.
  - In regions that are susceptible to electrical storms, we recommend that you plug your system into a surge suppressor.
  - Install equipment into the lower half of the rack first to avoid making the rack top heavy.
  - Ensure at least 3 inches clearance on all sides for effective ventilation. Do not obstruct the air intake vent on the front, side, or rear ventilation grills. Locate the system away from heat sources.
- Ensure that your equipment is placed in an area that accommodates the power consumption and component heat dissipation specifications.
- Ensure that your power supplies meet the site power or AC power requirements of the all network equipment.
- Extreme products are class A digital devices compliant with FCC Part 15, and other class A international standards. Operation is subjective to the following. (1) This device may cause harmful interference, and (2) this device must accept any interference received including interference that may cause undesirable operation.

Installing Power Supply Units

WARNING!

Ensure that the following requirements are satisfied when installing all Extreme Networks power supplies. See Installation instructions of power supply unit (PSU) in questions for ratings and power requirements.

Make sure to satisfy the following requirements:

- Plug power supplies only into properly grounded electrical outlets to help prevent electrical shock and comply with international safety standards.
- Use only power cords that are certified for use within the country of use. Do not attempt to modify AC power cord.
- The wall outlet must be installed near the equipment and be easily accessible for quick disconnect.
- Make sure the voltage and frequency of your power outlet match the equipment's system's electrical ratings. The building and/or power source must provide overload protection.
- Use a surge suppressor, line conditioner, or uninterruptible power supply to protect the system from momentary increases or decreases in electrical power.
- For hot-swappable power supplies, do not slam PSU into the bay.
- If multiple power supplies are used in a switch, connect each power supply to different, independent power sources. If a single power source fails, it will affect only that power supply to which it is connected. If all the power supplies on a single switch are connected to the same power source, the entire switch is vulnerable to a power failure.

Power Input Requirements

AC Power Supply Input (Per input):

Voltage Input Range	90 – 264 V~
Nominal Input Voltage/Hz	115 V~/60Hz & 230 V~/50Hz
Line Frequency Range	47 – 63 Hz
Nominal Input Current	4.0 A @ 115 V~ (low-line) 2.0 A @ 230 V~ (high-line)
Maximum In-Rush Current	30A @ 120V~ / 60A @ 240V~ (Cold Start)
Efficiency	70% typical at 110VAC, 74% typical at 220V~ (Fill Load)
Power Supply Input Socket	IEC 320 C14
Power Cord Input Plug	IEC 320 C13
Power Cord Wall Plug	Please refer to "Power Supply Cords Selection" on page 13.
Minimum Wire Size	18 AWG (.82mm2) copper stranded

Maintenance Safety

Take the following precautions:

- Use only original accessories and/or components approved for use with this system. Failure to observe these instructions may damage the equipment or even violate required safety and EMC regulations.
- The chassis cover should only be removed by Extreme Networks personnel. There are no customer serviceable components in this system. Repairs to the system must be performed by an Extreme Networks factory service technician.
- The power on button for the system may not turn off all system power. To remove power from the system, you must unplug the all power cords from wall outlets. The power cord is the disconnect device to the main power source.
- Disconnect all power before removing the back panel of any Extreme Networks switch.
- Disconnect all power cords before working near power supplies unless otherwise instructed by a maintenance procedure.
- When handling modules, optic devices, power supplies, or other modular accessories put on the ESD-preventive wrist strap to reduce the risk of electronic damage to the equipment. Leave the electrostatic ally sensitive device (ESD)-preventive wrist strap permanently attached to the chassis so that it is always available when you need to handle ESD-sensitive components.
- Ensure that all cables are installed in a manner to avoid strain. Use tie wraps or other strain relief devices.
- Replace power cord immediately if it shows any signs of damage.

General Safety Precautions

Ensure that you conform to the following guidelines:

- Do not attempt to lift objects that you think are too heavy for you.
- When installing in rack, caution should be taken to load heavier devices in lowest portions of rack to avoid a top heavy hazard.
- For Summit desktop switches, do not place a monitor or other objects on top of the equipment. The chassis cover is not designed to support weight.
- Only use tools and equipment that are in perfect condition. Do not use equipment with visible damage.
- Protecting ESD--To protect ESDs always wear a wristband before carrying out any work on PC boards and modules. Transport PC boards only in electrostatic packaging. Always place PC boards on a grounded surface before working on them.
- Laying cables--Lay cables so as to prevent any risk of these cables being damaged or causing accidents, such as tripping.

Power Supply Cords Selection

Depending on the switch purchased, Extreme Networks AC power supply units (PSUs) come with only a 110 VAC cord or both a 110 VAC and 208/220 VAC power supply cords. The power supply cords provided by Extreme Networks are designed and certified for use in the United States and Canada only.

Power supply cords for use outside of United States and Canada are typically provided by a third-party distribution center and must meet the following requirements:

- Power supply cords must be agency certified for country of use.
- Power supply cords must contain an appropriate rated and approved wall plug applicable to the country of installation.
- The appliance coupler (the connector to the unit and not the wall plug) must have a configuration for mating with an EN60320/IEC320-C14 appliance inlet.
- Power supply cords must be less then 15ft (5m) long.
- The minimum specification for the flexible cable is:
  - No. 18 AWG (.823mm2) for units rated less than 10A, or
  - No. 18 AWG (.823mm2) up to 2m long for units rated 10A or higher, or
  - No. 16 AWG (1.0 mm2) up to 5m long for units rated 10A or higher
- All cords should be copper stranded, Type SVT or SJT, HAR or equivalent, 3-conductor.

Always use an AC power cable appropriate for your country. Check your local electrical codes and regulatory agencies for power cable requirements. Refer to Data Sheet of PSU at http://www.extremenetworks.com or Appendix B of this document for details of power specifications.

WARNING!

Ensure that the source outlet is properly grounded before plugging the AC supply power cord into a PSU.

Note the following country specific requirements:

- Argentina—The supply plug must comply with Argentinean standards.
- Australia—10 A minimum service receptacle, AS 3112 for 110/220 VAC power supplies.
- Denmark—The supply plug must comply with section 107-2-D1, standard DK2-1a or DK2-5a.
- Japan:
  - 10 A service receptacle, JIS 8303 for 110/220 VAC power supplies.
  - The power cord provided with the power supply, switch, or chassis is for use only with that specific product from Extreme Networks; it is not for use with any other product from Extreme Networks or any other vendors' equipment.
- North America—10 A service receptacle, NEMA 5-15 for 110 VAC power supplies and NEMA L6-15P for 208/220 V AC power supplies.
- Switzerland—The supply plug must comply with SEV/ASE 1011.
- United Kingdom—10 A service receptacle, BS 1363 for 110/220 VAC power supplies.
- International—10 A service receptacle, CEE 7/7 for 110/220 VAC power supplies.
- France and Peru only:

  This unit cannot be powered from IT† supplies. If your supplies are of IT type, this unit must be powered by 230 V (2P+T) via an isolation transformer ratio 1:1, with the secondary connection point labeled Neutral and connected directly to ground.

NOTE

Building codes vary worldwide; therefore, Extreme Networks strongly recommends that you consult an electrical contractor to ensure proper equipment grounding and power distribution for your specific installation.

Battery Replacement and Disposal

Please note the following for batteries:

- Replacing lithium battery--Batteries contained in this unit are not user-replaceable. Contact your Extreme Service personal for complete product replacement.

WARNING!

If replacement is attempted, the following guidelines must be followed to avoid danger of explosion:

1. replaced with the same or equivalent type as recommended by the battery manufacturer.
2. dispose of the battery in accordance with the battery manufacturer's recommendation.

Sicherheitshinweise

WARNUNG!

Vor der Installation der Produkte von Extreme Networks sind die nachfolgenden Sicherheitshinweise aufmerksam zu lesen. Die Nichtbeachtung dieser Sicherheitshinweise kann zu Verletzungen oder Schäden an der Ausrüstung führen.

Installation, Wartung und Ausbau eines Switch, einer Grundplatte oder einer seiner Komponenten dürfen nur von geschultem und qualifiziertem Servicepersonal durchgeführt werden! Geschulte und qualifizierte Servicetechniker verfügen über die erforderliche technische Ausbildung und Erfahrung, um mögliche Gefahren bei der Durchführung von Servicearbeiten zu erkennen und Maßnahmen zur Minimierung der Gefahr für sich bzw. andere zu treffen.

Hinweise zur Installation

WARNUNG!

Beachten Sie vor der Installation der Ausrüstung folgende Punkte.

Stellen Sie sicher, dass die nachfolgend aufgeführten Bedingungen erfüllt sind:

- Das System ist für den Einsatz in einer typischen Umgebung gemäß Telco-Vorgaben vorgesehen. Wählen Sie einen Aufstellort mit den folgenden Eigenschaften:
    - Innenbereich mit Temperatur- und Feuchtigkeitsregelung, wobei die maximale Raumtemperatur 40°C (104°F) nicht überschreiten darf.
    - Sauber und frei von elektrisch aufladbaren Teilchen in der Luft.
    - Ausreichende Belüftung und Abstand zu Wärmequellen, einschließlich direktem Sonnenlicht
    - Ausreichender Abstand zu Quellen, die Erschütterungen oder Schläge/Stöße hervorrufen können
    - Isolierung von starken elektromagnetischen Feldern, wie sie durch Elektrogeräte erzeugt werden
    - Sicherer, abgeschlossener Arbeitsbereich mit beschränktem Zugang, sodass nur geschultes und qualifiziertes Servicepersonal Zugriff auf das Gerät hat
    - In für elektrische Stürme anfälligen Gebieten wird empfohlen, das System an einen Spannungsstoßunterdrücker anzuschließen.
    - Die Ausrüstung im unteren Teil des Gestells installieren, um zu vermeiden, dass der obere Teil des Gestells zu schwer wird.
    - Auf allen Seiten für mindestens 7,5 cm (3“) Abstand sorgen, um eine ausreichende Belüftung zu gewährleisten. Die Lufteinlassöffnung an den vorderen, seitlichen und hinteren Entlüftungsgittern nicht blockieren. Das System nicht in der Nähe von Wärmequellen aufstellen.
- Sicherstellen, dass die Ausrüstung in einem Bereich aufgestellt wird, der den Spezifikationen für Leistungsaufnahme und Wärmeabstrahlung der Komponenten entspricht.
- Sicherstellen, dass Ihre Netzteile die Anforderungen an die Strom- oder Wechselstromversorgung vor Ort für alle Netzwerkgeräte erfüllen.
- Bei den Extreme-Produkten handelt es sich um digitale Geräte der Klasse A gemäß Teil 15 der FCC-Richtlinien und anderen internationalen Richtlinien. Der Gerätebetrieb unterliegt den folgenden Voraussetzungen: (1) Das Gerät kann schädliche Interferenzen verursachen, und (2) das Gerät muss

jede empfangene Interferenz zulassen, einschließlich einer Interferenz, die einen unerwünschten Betrieb verursachen kann.

Installation von Netzteilen

WARNUNG!

Bei der Installation sämtlicher Netzteile von Extreme Networks muss sichergestellt werden, dass die nachfolgend aufgeführten Anforderungen erfüllt sind. Angaben zu Nennleistung und Leistungsbedarf finden sich in den Installationsanweisungen für das jeweilige Netzteil (Power Supply Unit, PSU).

Folgende Anforderungen müssen unbedingt erfüllt sein:

- Netzteile nur an vorschriftsmäßig geerdete Steckdosen anschließen, um die Gefahr elektrischer Schläge zu vermeiden und die Konformität mit internationalen Sicherheitsnormen zu gewährleisten.
- Nur Stromkabel verwenden, die für den Einsatz in dem jeweiligen Land zugelassen sind. Wechselstromkabel dürfen nicht manipuliert werden.
- Die Wandsteckdose muss in der Nähe der Anlage installiert und leicht zugänglich sein, um eine schnelle Trennung vom Netz zu ermöglichen.
- Spannung und Frequenz der Steckdose müssen den elektrischen Nenndaten des Systems entsprechen. Das Gebäude bzw. die Stromquelle muss mit einem Überlastschutz ausgestattet sein.
- Einen Spannungsstoßunterdrücker, einen Netzfilter oder eine unterbrechungsfreie Stromversorgung verwenden, um das System vor einer vorübergehenden Zu- oder Abnahme der elektrischen Leistung zu schützen.
- Bei laufendem Betrieb austauschbare Netzteile: Das Netzteil vorsichtig, nicht mit Kraft in das Aufnahmefach einsetzen.
- Bei Einsatz mehrer Netzteile in einem Switch sind die Netzteile jeweils an unterschiedliche, unabhängige Stromquellen anzuschließen. Auf diese Weise ist bei einem Ausfall einer einzelnen Stromquelle nur das daran angeschlossene Netzteil betroffen. Wenn alle Netzteile eines einzelnen Switch an dieselbe Stromquelle angeschlossen sind, ist der gesamte Switch für einen Ausfall der Stromversorgung anfällig.

Leistungsspezifikationen für Netzteile von Extreme Networks finden sich in Anhang B dieses Dokuments oder im Netzteil-Datenblatt unter http://www.extremenetworks.com.

Wartungssicherheit

Folgende Vorsichtsmaßnahmen müssen getroffen werden:

- Nur für den Einsatz mit diesem System zugelassene Originalzubehörteile bzw. -komponenten verwenden. Die Nichtbeachtung dieser Anweisungen kann zu Schäden an der Ausrüstung oder sogar zu einem Verstoß gegen die erforderlichen Sicherheitsbestimmungen und EMV-Vorschriften führen.
- Die Abdeckung der Grundplatte darf nur durch Personal von Extreme Networks entfernt werden. Das System enthält keine vom Kunden zu wartenden Komponenten. Reparaturen am System sind von einem Werkstechniker von Extreme Networks durchzuführen.
- Der An-/Aus-Schalter des Systems darf nicht die gesamte Stromversorgung zum System unterbrechen. Zur Unterbrechung der Wechselstromversorgung zum System müssen alle Stromkabel

aus den Wandsteckdosen gezogen werden. Das Stromkabel dient zur Trennung von der Netzstromversorgung.

- Vor dem Entfernen der Rückwand eines Extreme Networks-Switch muss die gesamte Stromzufuhr unterbrochen werden.
- Vor der Aufnahme von Arbeiten in der Nähe von Stromquellen alle Stromkabel abziehen, sofern nicht im Rahmen eines Wartungsverfahrens anders vorgegeben.
- Beim Umgang mit Modulen, optischen Geräten, Netzteilen oder anderen modularen Zubehörteilen das ESD-Schutzarmband anlegen, um das Risiko einer Beschädigung der Geräte durch elektrostatische Entladungen zu verringern. Das Armband zum Schutz elektrostatisch gefährdeter Bauteile (ESB) grundsätzlich an der Grundplatte befestigt lassen, damit es beim Umgang mit diesen Bauteilen immer zur Hand ist.
- Alle Kabel so verlegen, dass übermäßige Belastungen vermieden werden. Kabelbinder oder Zugentlastungsklemmen verwenden.
- Ein Stromkabel bei Anzeichen von Beschädigungen unverzüglich austauschen.

Allgemeine Sicherheitsvorkehrungen

Folgende Richtlinien sind unbedingt zu befolgen:

- Keine Gegenstände heben, die möglicherweise zu schwer sind.
- Bei einer Installation in einem Gestell darauf achten, dass schwere Geräte unten im Gestell eingebaut werden, um Gefahren durch Umkippen zu vermeiden.
- Bei Summit Desktop-Switches keinen Monitor oder andere Gegenstände auf die Anlage stellen. Die Abdeckung der Grundplatte ist nicht darauf ausgelegt, Gewicht zu tragen.
- Nur Werkzeuge und Ausrüstung verwenden, die sich in einwandfreiem Zustand befinden. Keine Ausrüstung verwenden, die sichtbare Beschädigungen aufweist.
- Schutz ESD-gefährdeter Bauteile: Zum Schutz ESD-gefährdeter Bauteile grundsätzlich vor der Aufnahme von Arbeiten an Leiterplatten oder Modulen ein Armband anlegen. Leiterplatten nur in antistatischer Verpackung transportieren. Vor der Aufnahme von Arbeiten an Leiterplatten diese immer auf einer geerdeten Fläche ablegen.
- Verlegen von Kabeln: Kabel so verlegen, dass keine Schäden entstehen oder Unfälle, z. B. durch Stolpern, verursacht werden können.

Auswahl der Stromkabel

Je nachdem, welchen Switch Sie erworben haben, werden die Wechselstromnetzteile von Extreme Networks entweder nur mit einem 110-VAC-Kabel oder mit einem 110-VAC-Kabel und einem 208/220-VAC-Kabel geliefert. Die von Extreme Networks gelieferten Stromkabel sind nur für den Einsatz in den Vereinigten Staaten und Kanada ausgelegt und zugelassen. Stromkabel für den Einsatz außerhalb der Vereinigten Staaten und Kanada werden normalerweise von einem Drittanbieter geliefert und müssen die folgenden Anforderungen erfüllen:

- Die Stromkabel müssen offiziell für das Land zugelassen sein, in dem sie verwendet werden sollen.
- Die Stromkabel müssen mit einem für das Einsatzland zugelassenen Wandsteckkontakt mit der geeigneten Nennleistung ausgerüstet sein.
- Die Konfiguration der Steckvorrichtung (die Steckverbindung zur Einheit, nicht zur Wandsteckdose) muss für eine Gerätesteckdose gemäß EN60320/IEC320-C14 ausgeführt sein.

- Die Länge der Stromkabel muss weniger als 5 m (15 Fuß) betragen.
- Die Mindestspezifikation für das flexible Kabel lautet:
  - Nr. 18 AWG (0,823 mm^2) für Einheiten mit einem Bemessungsstrom von weniger als 10 A, oder
  - Nr. 18 AWG (0,823 mm^2) bis 2 m Länge für Einheiten mit einem Bemessungsstrom von 10 A oder höher, oder
  - Nr. 16 AWG (1,0 mm^2) bis 5 m Länge für Einheiten mit einem Bemessungsstrom von 10 A oder höher
- Bei allen Kabeln muss es sich um 3-adrige Kupferleiter vom Typ SVT oder SJT, HAR oder einen äquivalenten Typ handeln.

Verwenden Sie immer ein Wechselstromkabel, das den Vorschriften Ihres Landes entspricht. Erkundigen Sie sich über die örtlichen Vorschriften für Elektroinstallationen und fragen Sie bei den zuständigen Aufsichtsbehörden nach den Anforderungen an Stromkabel. Nähere Angaben zu den Leistungsspezifikationen von Netzteilen finden sich unter http://www.extremenetworks.com.

WARNUNG!

Vor dem Anschließen des Wechselstromkabels an ein Netzteil muss sichergestellt werden, dass die Steckdose vorschriftsgemäß geerdet ist.

HINWEIS

Die Bauvorschriften sind weltweit verschieden; Extreme Networks empfiehlt daher ausdrücklich, einen Elektroinstallateur zu beauftragen, um die sachgemäße Geräteerdung und Stromverteilung für Ihre spezifische Installation sicherzustellen.

Austauschen und Entsorgen von Batterien

Im Umgang mit Batterien sind folgende Hinweise zu beachten:

- Austauschen der Lithium-Batterie: Die in diesem Gerät enthaltenen Batterien können nicht vom Anwender ausgetauscht werden. Wenden Sie sich für einen Austausch des kompletten Gerätes bitte an die Servicemitarbeiter von Extreme. Sollte der Versuch eines Austausches unternommen werden, sind zur Vermeidung einer Explosionsgefahr folgende Richtlinien zu beachten:
  - 1) Die Batterie nur durch eine identische oder eine gleichwertige, vom Hersteller empfohlene Batterie ersetzen.
  - 2) Die Batterie gemäß den Empfehlungen des Herstellers entsorgen.

Die deutsche Version der für dieses Produkt von Extreme Networks relevanten Sicherheitshinweise finden sich im Abschnitt „Sicherheitshinweise“ im Summit WM Series WLAN Switch and Altitude Access Point Software Version 4.1 User Guide. Dieses Installationshandbuch steht auf der folgenden Webseite zum Download zur Verfügung: http://www.extremenetworks.com/services/documentation/hwuserguides.asp. oder gefunden auf beiliegender CD.

1 Overview of the Summit WM series switch, access points, and WLAN switch software solution

This chapter describes Summit WM series switch, access points, and WLAN switch software concepts, including:

- Conventional wireless LANs
- Elements of the Summit WM series switch, access points, and WLAN switch software solution
- Summit WM series switch, access points, and WLAN switch software and your network
- System Configuration Overview

The next generation of Extreme Networks wireless networking devices provides a truly scalable WLAN solution. Extreme Networks Altitude APs are fit access points controlled through a sophisticated network device, the Summit WM series switch. This solution provides the security and manageability required by enterprises and service providers.

The Summit WM series switch, access points, and WLAN switch software system is a highly scalable Wireless Local Area Network (WLAN) solution developed by Extreme Networks. Based on a third generation WLAN topology, the Summit WM series switch, access points, and WLAN switch software system makes wireless practical for service providers as well as medium and large-scale enterprises.

The Summit WM series switch, access points, and WLAN switch software system provides a secure, highly scalable, cost-effective solution based on the IEEE 802.11 standard. The system is intended for enterprise networks operating on multiple floors in more than one building, and is ideal for public environments, such as airports and convention centers that require multiple access points.

This chapter provides an overview of the fundamental principles of the Summit WM series switch, access points, and WLAN switch software system.

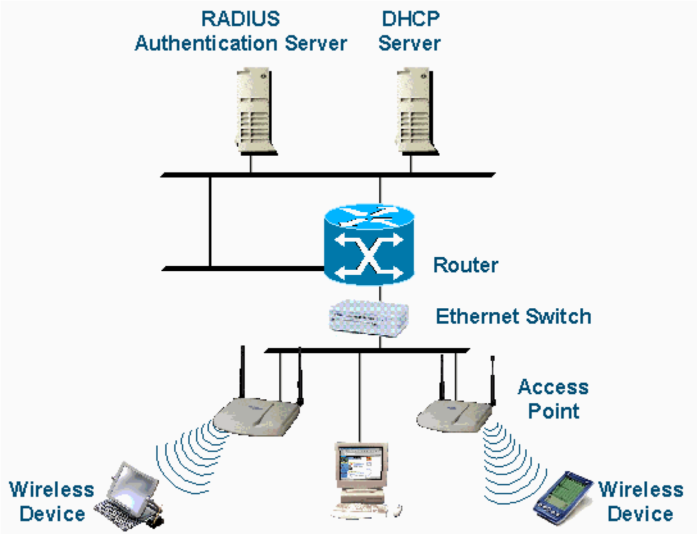
Conventional wireless LANs

Wireless communication between multiple computers requires that each computer is equipped with a receiver/transmitter—a WLAN Network Interface Card (NIC)—capable of exchanging digital information over a common radio frequency. This is called an ad hoc network configuration. An ad hoc network configuration allows wireless devices to communicate together. This setup is defined as an independent basic service set (IBSS).

An alternative to the ad hoc configuration is the use of an access point. This may be a dedicated hardware bridge or a computer running special software. Computers and other wireless devices communicate with each other through this access point. The 802.11 standard defines access point communications as devices that allow wireless devices to communicate with a distribution system. This setup is defined as a basic service set (BSS) or infrastructure network.

To allow the wireless devices to communicate with computers on a wired network, the access points must be connected to the wired network providing access to the networked computers. This topology is called bridging. With bridging, security and management scalability is often a concern.

Figure 1: Standard wireless network solution example



The wireless devices and the wired networks communicate with each other using standard networking protocols and addressing schemes. Most commonly, Internet Protocol (IP) addressing is used.

Elements of the Summit WM series switch, access points, and WLAN switch software solution

The Summit WM series switch, access points, and WLAN switch software solution consists of two devices:

- Summit WM series switch
- Altitude APs

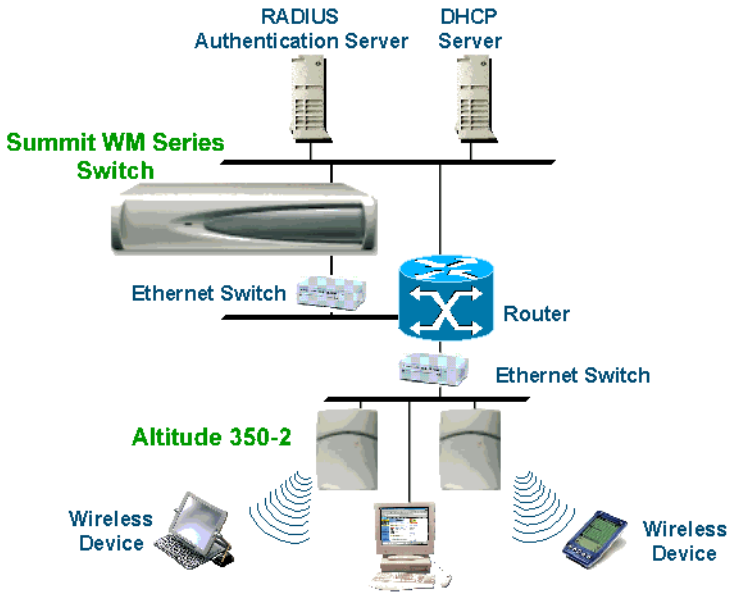
This architecture allows a single Summit WM series switch to control many Altitude APs, making the administration and management of large networks much easier.

There can be several Summit WM series switches in the network, each with a set of registered Altitude APs. The Summit WM series switches can also act as backups to each other, providing stable network availability.

In addition to the Summit WM series switches and Altitude APs, the solution requires three other components, all of which are standard for enterprise and service provider networks:

- RADIUS Server (Remote Access Dial-In User Service) or other authentication server
- DHCP Server (Dynamic Host Configuration Protocol)
- SLP (Service Location Protocol)

Figure 2: Extreme Networks solution



As illustrated in Figure 2, the Summit WM series switch appears to the existing network as if it were an access point, but in fact one Summit WM series switch controls many Altitude APs.

The Summit WM series switch has built-in capabilities to recognize and manage the Altitude APs. The Summit WM series switch:

- Activates the Altitude APs
- Enables Altitude APs to receive wireless traffic from wireless devices
- Processes the data traffic from the Altitude APs
- Forwards or routes the processed data traffic out to the network
- Authenticates requests and applies access policies

Simplifying the Altitude APs makes them cost-effective, easy to manage, and easy to deploy. Putting control on an intelligent centralized Summit WM series switch enables:

- Centralized configuration, management, reporting, and maintenance
- High security
- Flexibility to suit enterprise
- Scalable and resilient deployments with a few Summit WM series switches controlling hundreds of Altitude APs

The Summit WM series switch, access points, and WLAN switch software system:

- **Scales up to Enterprise capacity –** One Summit WM series switch WM2000 controls as many as 200 Altitude APs. In turn each Altitude AP can handle up to 254 wireless devices, with each radio supporting a maximum of 128. With additional Summit WM series switches, the number of wireless devices the solution can support can reach into the thousands.
- **Integrates with existing network –** A Summit WM series switch can be added to an existing enterprise network as a new network device, greatly enhancing its capability without interfering with existing functionality. Integration of the Summit WM series switches and Altitude APs does not require any reconfiguration of the existing infrastructure (for example, VLANs).

- **Offers centralized management and control –** An administrator accesses the Summit WM series switch in its centralized location to monitor and administer the entire wireless network. From the Summit WM series switch the administrator can recognize, configure, and manage the Altitude APs and distribute new software releases.
- **Provides easy deployment of Altitude APs** – The initial configuration of the Altitude APs on the centralized Summit WM series switch can be done with an automatic "discovery" technique. For more information, see "Discovery and registration overview" on page 56.
- **Provides security via user authentication –** Uses existing authentication (AAA) servers to authenticate and authorize users.
- **Provides security via filters and privileges –** Uses virtual networking techniques to create separate virtual networks with defined authentication and billing services, access policies, and privileges.
- **Supports seamless mobility and roaming** – Supports seamless roaming of a wireless device from one Altitude AP to another on the same Summit WM series switch or on a different Summit WM series switch.
- **Integrates third-party access points –** Uses a combination of network routing and authentication techniques.
- **Prevents rogue devices –** Unauthorized access points are detected and identified as harmless or dangerous rogue APs.
- **Provides accounting services –** Logs wireless user sessions, user group activity, and other activity reporting, enabling the generation of consolidated billing records.
- **Offers troubleshooting capability –** Logs system and session activity and provides reports to aid in troubleshooting analysis.
- **Offers dynamic RF management –** Automatically selects channels and adjusts Radio Frequency (RF) signal propagation and power levels without user intervention.

Summit WM series switch, access points, and WLAN switch software and your network

This section is a summary of the components of the Summit WM series switch, access points, and WLAN switch software solution on your enterprise network. The following are described in detail in this guide, unless otherwise stated:

- **Summit WM series switch** – A rack-mountable network device that provides centralized control over all access points (both Altitude APs and third-party access points) and manages the network assignment of wireless device clients associating through access points.
- **Altitude AP** - A wireless LAN fit access point (IEEE 802.11) that communicates only with a Summit WM series switch.
- **RADIUS Server** (Remote Access Dial-In User Service) (RFC2865), or other authentication server – An authentication server that assigns and manages ID and Password protection throughout the network. Used for authentication of the wireless users in either 802.1x or Captive Portal security modes. The RADIUS Server system can be set up for certain standard attributes, such as filter ID, and for the Vendor Specific Attributes (VSAs). In addition, Radius Disconnect (RFC3576) which permits dynamic adjustment of user policy (user disconnect) is supported.
- **DHCP Server** (Dynamic Host Configuration Protocol) (RFC2131) – A server that assigns IP addresses, gateways, and subnet masks dynamically. IP address assignment for clients can be done by the DHCP server internal to the Summit WM series switch, or by existing servers using DHCP relay. It is also used by the Altitude APs to discover the location of the Summit WM series switch

during the initial registration process. For SLP, DHCP should have Option 78 enabled. Option 78 specifies the location of one or more SLP Directory Agents.

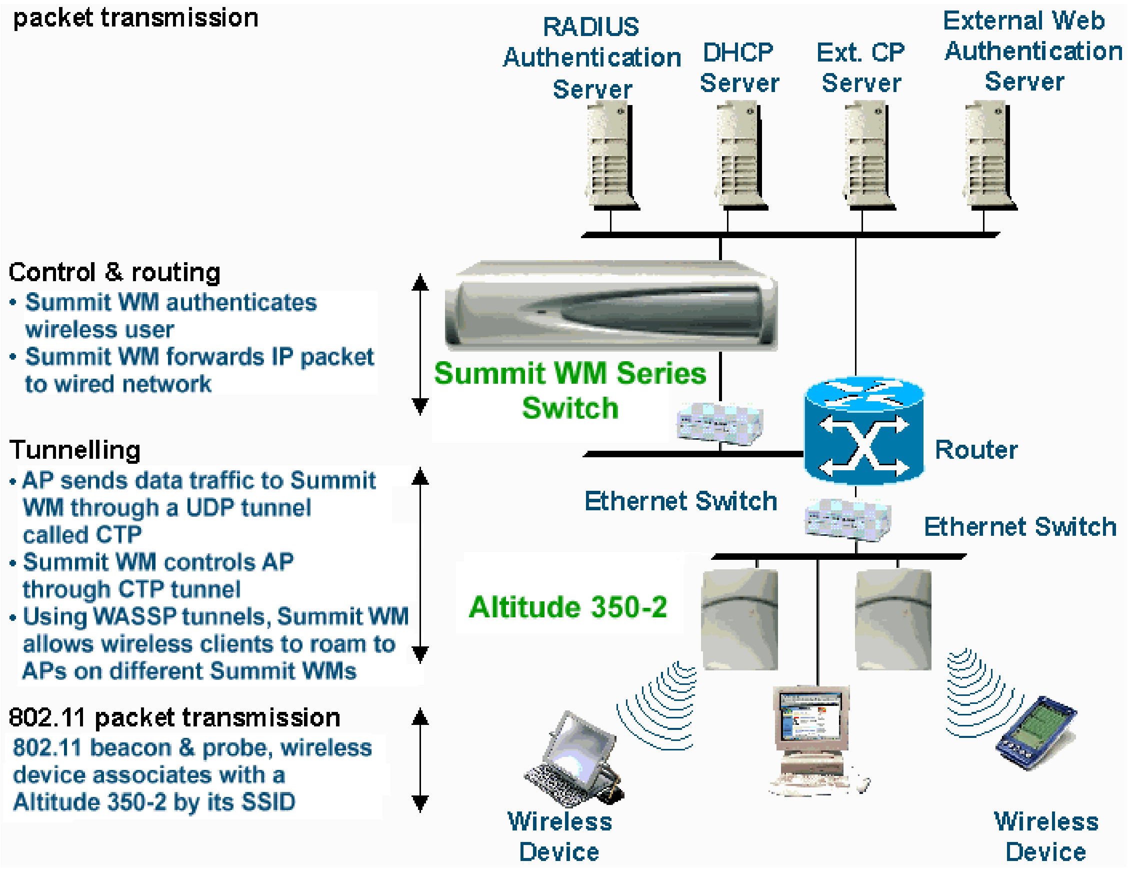
- **Service Location Protocol (SLP)** (SLP RFC2608) – Client applications are User Agents and services that are advertised by a Service Agent. In larger installations, a Directory Agent collects information from Service Agents and creates a central repository. The Extreme Networks solution relies on registering “extreme” as an SLP Service Agent.
- **Domain Name Server (DNS)** – A server used as an alternate mechanism (if present on the enterprise network) for the automatic discovery process. Summit WM series switch, access points, and WLAN switch software relies on the DNS for Layer 3 deployments and for static configuration of Altitude APs. The controller can be registered in DNS, to provide DNS assisted AP discovery.
- **Web Authentication Server** – A server that can be used for external Captive Portal and external authentication. The Summit WM series switch has an internal Captive portal presentation page, which allows Web authentication (Web redirection) to take place without the need for an external Captive Portal server.
- **RADIUS Accounting Server** (Remote Access Dial-In User Service) (RFC2866) – A server that is required if RADIUS Accounting is enabled.
- **Simple Network Management Protocol (SNMP)** – A Manager Server that is required if forwarding SNMP messages is enabled.
- **Check Point Server** (Check Point Event Logging API) – A server for security event logging that is required if a firewall application is enabled. Checkpoint ELA certification for OPSEC is provided.
- **Network infrastructure** – The Ethernet switches and routers must be configured to allow routing between the various services noted above. Routing must also be enabled between multiple Summit WM series switches for the following features to operate successfully:
  - Availability
  - Mobility
  - Summit spy for detection of rogue access points

    Some features also require the definition of static routes.
- **Web Browser** – A browser provides access to the Summit WM series switch Management user interface to configure the Summit WM series switch, access points, and WLAN switch software.
- **SSH Enabled Device** – A device that supports Secure Shell (SSH) is used for remote (IP) shell access to the system.
- **Zone Integrity** – The Zone integrity server enhances network security by ensuring clients accessing your network are compliant with your security policies before gaining access. Zone Integrity Release 5 is supported.

Network traffic flow

Figure 3 illustrates a simple configuration with a single Summit WM series switch and two Altitude APs, each supporting a wireless device. A RADIUS server on the network provides authentication, and a DHCP server is used by the Altitude APs to discover the location of the Summit WM series switch during the initial registration process. Network inter-connectivity is provided by the infrastructure routing and switching devices.

Figure 3: Traffic Flow diagram


packet transmission
RADIUS Authentication Server
DHCP Server
Ext. CP Server
External Web Authentication Server
Control & routing
• Summit WM authenticates wireless user
• Summit WM forwards IP packet to wired network
Summit WM Series Switch
Router
Tunnelling
• AP sends data traffic to Summit WM through a UDP tunnel called CTP
• Summit WM controls AP through CTP tunnel
• Using WASSP tunnels, Summit WM allows wireless clients to roam to APs on different Summit WMs
Ethernet Switch
Ethernet Switch
Altitude 350-2
802.11 packet transmission
802.11 beacon & probe, wireless device associates with a Altitude 350-2 by its SSID
Wireless Device
Wireless Device

Each wireless device sends IP packets in the 802.11 standard to the Altitude AP. The Altitude AP uses a UDP (User Datagram Protocol) based tunnelling protocol to encapsulate the packets and forward them to the Summit WM series switch. In a typical configuration, access points can be configured to locally bridge traffic (to a configured VLAN) directly at their network point of attachment. The Summit WM series switch decapsulates the packets and routes these to destinations on the network.

The Summit WM series switch functions like a standard router, except that it is configured to route only network traffic associated with wireless connected users. The Summit WM series switch can also be configured to simply forward traffic to a default or static route if dynamic routing is not preferred.

Network security

The Summit WM series switch, access points, and WLAN switch software system provides features and functionality to control network access. These are based on standard wireless network security practices.

Current wireless network security methods provide protection. These methods include:

- Shared Key authentication that relies on Wired Equivalent Privacy (WEP) keys
- Open System that relies on Service Set Identifiers (SSIDs)
- 802.1x that is compliant with Wi-Fi Protected Access (WPA)
- Captive Portal based on Secure Sockets Layer (SSL) protocol

The Summit WM series switch, access points, and WLAN switch software system provides the centralized mechanism by which the corresponding security parameters are configured for a group of APs.

- Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks defined in the 802.11b standard
- Wi-Fi Protected Access version 1 (WPA1™) with Temporal Key Integrity Protocol (TKIP)
- Wi-Fi Protected Access version 2 (WPA2™) with Advanced Encryption Standard (AES) and Counter Mode with Cipher Block Chaining Message Authentication Code (CCMP)

Authentication

The Summit WM series switch relies on a RADIUS server, or authentication server, on the enterprise network to provide the authentication information (whether the user is to be allowed or denied access to the network). A RADIUS client is implemented to interact with infrastructure RADIUS servers.

The Summit WM series switch provides authentication using:

- Captive Portal – a browser-based mechanism that forces users to a Web page
- RADIUS (using IEEE 802.1x)

The 802.1x mechanism is a standard for authentication developed within the 802.11 standard. This mechanism is implemented at the wireless Port, blocking all data traffic between the wireless device and the network until authentication is complete. Authentication by 802.1x standard uses Extensible Authentication Protocol (EAP) for the message exchange between the Summit WM series switch and the RADIUS server.

When 802.1x is used for authentication, the Summit WM series switch provides the capability to dynamically assign per-wireless-device WEP keys (called per-station WEP keys in 802.11). Or in the case of WPA, the Summit WM series switch is not involved in key assignment. Instead, the controller is involved in the path between RADIUS server and the user to negotiate the appropriate set of keys. With WPA2 the material exchange produces a Pairwise Master Key which is used by the AP and the user to derive their temporal keys. (The keys change over time.)

In the Summit WM series switch, access points, and WLAN switch software, a RADIUS redundancy feature is provided, where you can define a failover RADIUS server (up to 2 servers) in the event that the active RADIUS server fails.

Privacy

Privacy is a mechanism that protects data over wireless and wired networks, usually by encryption techniques.

Summit WM series switch, access points, and WLAN switch software supports the Wired Equivalent Privacy (WEP) standard common to conventional access points.

It also provides Wi-Fi Protected Access version 1 (WPA v.1) encryption, based on Pairwise Master Key (PMK) and Temporal Key Integrity Protocol (TKIP). The most secure encryption mechanism is WPA version 2, using Advanced Encryption Standard (AES).

WM Access Domain Services

WM Access Domain Services (WM-AD) provide a versatile method of mapping wireless networks to the topology of an existing wired network.

When you set up WM Access Domain Services (WM-AD) on the Summit WM series switch you are defining subnets for groups of wireless users. The WM-AD definition provides the binding between WM-AD IP topology configuration (Routing, DHCP policy) and the RF configuration parameters that advertise and control network access (SSID, Privacy policy: WEP and WPA). This technique enables policies and authentication to be applied to the groups of wireless users on a WM-AD, as well as the collecting of accounting information on user sessions that can be used for billing.

When a WM-AD is set up on the Summit WM series switch:

- One or more Altitude APs (by radio) are associated with it
- A range of IP addresses is set aside for the Summit WM series switch’s DHCP server to assign to wireless devices

If routing protocol is enabled, the Summit WM series switch advertises the WM-AD as a routable network segment to the wired network and routes traffic between the wireless devices and the wired network. The Summit WM series switch WM200/2000 also supports VLAN-bridged assignment for WM-ADs. This allows the controller to directly bridge the set of wireless devices associated with a WM-AD directly to a specified core VLAN. The Summit WM series switch WM200/2000 can support up to 64 WM-ADs.

The AP radios can be assigned to each of the configured WM-ADs in a system. Each AP can be the subject of 8 WM-AD assignments (corresponding to the number of SSIDs it can support). Once a radio has all 8 slots assigned, it is no longer eligible for further assignment.

Static routing and routing protocols

Routing can be used on the Summit WM series switch to support the WM-AD definitions. Through the user interface you can configure routing on the Summit WM series switch to use one of the following routing techniques:

- **Static routes** – Use static routes to set the default route of a Summit WM series switch so that legitimate wireless device traffic can be forwarded to the default gateway.
- **Open Shortest Path First** (OSPF, version 2) (RFC2328) – Use OSPF to allow the Summit WM series switch to participate in dynamic route selection. OSPF is a protocol designed for medium and large IP networks with the ability to segment routes into different areas by routing information summarization and propagation. Static Route definition and OSPF dynamic learning can be combined, but a static route definition will take precedence over dynamic rules.
- **Next-hop routing** – Use next-hop routing to specify a unique gateway to which traffic on a WM-AD is forwarded. Defining a next-hop for a WM-AD forces all the traffic in the WM-AD to be forwarded to the indicated network device, bypassing any routing definitions of the controller's route table.

Packet filtering policy

Policy refers to the rules that allow different groups of users access to the network. The Summit WM series switch, access points, and WLAN switch software system can link authorized users to user groups. These user groups then can be confined to predefined portions of the network.

In the Summit WM series switch, access points, and WLAN switch software system, network access policy is carried out by means of packet filtering within a WM-AD.

In the Summit WM series switch user interface, you set up a packet filtering policy by defining a set of hierarchical rules that allow or deny traffic to specific IP addresses, IP address ranges, or service ports. The sequence and hierarchy of these filtering rules must be carefully designed based on your enterprise user access plan.

The authentication technique selected determines how filtering is carried out:

- If authentication is by SSID and Captive Portal, a non-authenticated filter allows all users to get as far as the Captive Portal Web page, where logon authentication occurs. When authentication is returned, then filters are applied, based on user ID and permissions.
- If authentication is by AAA (802.1x), users have logged on and have been authenticated before being assigned an IP address. When authentication is completed, the authenticated filter is assigned by default unless a more user-specific filter is returned or indicated by the authentication mechanism. The characteristics and level of access for a filter are controlled and defined by the system administrator.

Mobility and roaming

In typical configurations that are not Summit WM series switches, APs are setup as bridges that bridge wireless traffic to the local subnet. In bridging configurations, the user obtains an IP address from the same subnet as the AP. If the user roams within APs on the same subnet, it is able to keep using the same IP address. However, if the user roams to another AP outside of that subnet, its IP address is no longer valid. The user's client device must recognize that the IP address it has is no longer valid and re-negotiate a new one on the new subnet. The protocol does not mandate any action on the user. The recovery procedure is entirely client dependent. Some clients automatically attempt to obtain a new address on roam (which affects roaming latency), while others will hold on to their IP address. This loss of IP address continuity seriously affects the client's experience in the network, because in some cases it can take minutes for a new address to be negotiated.

The Summit WM series switch, access points, and WLAN switch software solution centralizes the user's network point of presence, therefore abstracting and decoupling the user's IP address assignment from that of the APs location subnet. That means that the user is able to roam across any AP without loosing its own IP address, regardless of the subnet on which the serving APs are deployed.

In addition, a Summit WM series switch can learn about other Summit WM series switches on the network and then exchange client session information. This enables a wireless device user to roam seamlessly between different Altitude APs on different Summit WM series switches.

Network availability

Summit WM series switch, access points, and WLAN switch software provides availability against Altitude AP outages, Summit WM series switch outages, and even network outages. The Summit WM series switch (WM200/2000 model) in a VLAN bridged WM-AD can potentially allow the user to retain the IP address in a failover scenario, if the WM-AD/VLAN is common to both controllers. For example, availability is provided by defining a paired controller configuration by which each peer can act as the backup controller for the other's APs. APs in one controller are allowed to failover and register with the alternate controller.

If a Summit WM series switch fails, all of its associated Altitude APs can automatically switch over to another Summit WM series switch that has been defined as the secondary or backup Summit WM series switch. If the AP reboots, the original Summit WM series switch is restored. The original Summit WM series switch is restored if it is active. However, active APs will continue to be attached to the failover controller until the administrator releases them back to the original home controller.

Quality of Service (QoS)

Summit WM series switch, access points, and WLAN switch software provides advanced Quality of Service (QoS) management to provide better network traffic flow. Such techniques include:

- **WMM (Wi-Fi Multimedia)** – WMM is enabled per WM-AD.The Summit WM series switch provides centralized management of these AP features. For devices with WMM enabled, the standard provides multimedia enhancements for audio, video, and voice applications. WMM shortens the time between transmitting packets for higher priority traffic. WMM is part of the 802.11e standard for QoS.
- **IP ToS (Type of Service)** or **DSCP (Diffserv Codepoint)** – The **ToS/DSCP** field in the IP header of a frame indicates the priority and QoS for each frame. The IP TOS and/or DSCP is maintained within CTP (CAPWAP Tunneling Protocol) by copying the user IP QoS information to the CTP header—this is referred to as Adaptive QoS.

Quality of Service (QoS) management is also provided by:

- Assigning high priority to an SSID (configurable)
- Adaptive QoS (automatic)
- Support for legacy devices that use SpectraLink Voice Protocol (SVP) for prioritizing voice traffic (configurable)

System Configuration Overview

To set up and configure the Summit WM series switch and Altitude APs, follow these steps:

1. First-time Setup – Perform "First-Time Setup" of the Summit WM series switch on the physical network to modify the Management Port IP address for the enterprise network.
2. Product Key – Apply a Product Key file, for licensing purposes. If no Product Key is enabled, the Summit WM series switch functions with some features enabled in demonstration mode. Not all features are enabled in this mode. For example, mobility is not enabled and cannot be used.
3. Data Port Setup – Set up the Summit WM series switch on the network by configuring the physical data ports and their function as "host port", "router port", or "3rd party AP port".
4. Routing Setup – Configure static routes and OSPF parameters for any port defined as a router port, if appropriate to the network.
5. Altitude AP Initial Setup – Connect the Altitude APs to the Summit WM series switch. They will automatically begin the Discovery of the Summit WM series switch, based on factors that include:
   - Their Registration mode (in the **Altitude AP Registration** screen)
   - The enterprise network services that will support the discovery process

     A new feature of the 4.0 release is a default AP configuration. The default AP configuration allows for a definition of a default configuration template, whereby APs automatically receive complete configuration. For typical deployments where all APs are to all have the same configuration, this feature will expedite deployment, as an AP will automatically receive full configuration (including WM-AD assignment) upon initial registration with the Summit WM series switch.

6 **Altitude AP Configuration – Modify properties or settings of the Altitude AP, if applicable.**

7 WM Access Domain Services (WM-AD) Setup – Set up one or more virtual subnetworks on the Summit WM series switch. For each WM-AD, configure the following:

- **Topology** – Configure the WM-AD.
- **RF** – Assign the Altitude APs' radios to the WM-AD.
- **Authentication and Accounting** – Configure the authentication method for the wireless device user and enable the accounting method.
- **RAD Policy** – Define filter ID values and WM-AD Groups
- **Filtering** – Define filtering rules to control network access
- **Multicast** – Define groups of IP addresses for multicast traffic
- **Privacy** – Select and configure the wireless security method on the WM-AD.
- **QoS Policy** – Configure the Qos Policy.

2 Configuring the Summit WM series switch

This chapter introduces the Summit WM series switch and describes the steps involved in its initial configuration and setup, including:

- System configuration overview
- Performing the first-time setup of the Summit WM series switch
- Completing the system configuration
- Ongoing Operations of the Summit WM series switch, access points, and WLAN switch software

The Summit WM series switch is a network device designed to integrate with an existing wired Local Area Network (LAN). The rack-mountable Summit WM series switch provides centralized management, network access, and routing to wireless devices that use Altitude APs to access the network. It can also be configured to handle data traffic from third-party access points.

The Summit WM series switch provides the following functionality:

- Controls and configures Altitude APs, providing centralized management
- Authenticates wireless devices that contact an Altitude AP
- Assigns each wireless device to a WM-AD when it connects
- Routes traffic from wireless devices, using WM-AD, to the wired network
- Applies filtering policies to the wireless device session
- Provides session logging and accounting capability

The Summit WM series switch is available in the following product families:

Table 1: Summit WM series switch product families

Summit WM series switch Model Number	Specifications
Summit WM200 (Enterprise license)	• Four GigE ports supporting up to 200 Altitude APs • One management port (10/100 BaseT) • One console port (DB9 serial) • Power supply standard (R)
Summit WM2000 (Campus license)	• Four GigE ports supporting up to 100 Altitude APs • One management port (10/100 BaseT) • One console port (DB9 serial) • Power supply standard (R)

System configuration overview

The following section provides a high-level overview of the steps involved in the initial configuration of your system:

Step 1 – Before you begin configuration

Research the type of WLAN deployment that is required.

Step 2 – Preparing the network

Ensure relevant DHCP servers and RADIUS servers (if applicable) are available and configured.

Step 3 – Installing the hardware

Install the Summit WM series switch WM200/2000. For more information, see the *Summit WM Series WLAN Switch Installation Instructions*.

Step 4 – Performing the first-time setup

Perform the first-time Setup of the Summit WM series switch on the physical network, which includes configuring the physical port IP:

- Configure the default IP address to be the relevant subnet point of attachment to the existing network. The default IP address is 10.0.#.1.
- Setup the routing protocol table.
- Configure the time zone, and then restart the Summit WM series switch. Because changing the time zone requires restarting the Summit WM series switch, it is recommended that you configure the time zone during the initial installation and configuration of the Summit WM series switch to avoid network interruptions. For more information, see "Configuring network time" on page 165.
- To configure a physical port to attach to a VLAN, define the VLAN as part of the IP address assignment.

Applying the product license key

Apply a product license key file. If a product license key is not applied, the Summit WM series switch functions with some features enabled in demonstration mode. Not all features are enabled in demonstration mode. For example, mobility is not enabled and cannot be used.

WARNING!

Whenever the licensed region changes on the Summit WM series switch, all Altitude APs are changed to Auto Channel Select to prevent possible infractions to local RF regulatory requirements. If this occurs, all manually configured radio channel settings will be lost.

Installing the new license key before upgrading will prevent the Summit WM series switch from changing the licensed region, and in addition, manually configured channel settings will be maintained. For more information, see "Performing Summit WM series switch software maintenance" on page 210.

Configuring for remote access

In addition, the first-time setup also involves configuring for remote access, which includes:

- Setting up an administration station (laptop) on subnet 192.168.10.0/24. By default, the controller's interface is configured with static IP 192.168.10.1.
- Configuring the system management interface.
- Configuring the data interfaces.

  Set up the Summit WM series switch on the network by configuring the physical data ports and their function as “host port”, “router port”, or “3rd party AP port”.
- Configure the routing table.

  Configure static routes or OSPF parameters for any port defined as a router port, if appropriate to the network.

For more information, see “Performing the first-time setup of the Summit WM series switch” on page 36.

Step 5 – Configuring the WM-AD

Research and then configure the traffic topologies your network must support. Set up one or more virtual subnetworks on the Summit WM series switch. For each WM-AD, configure the following:

- **Topology** – Configure the WM-AD.
- **RF** – Assign the Altitude APs’ radios to the WM-AD.
- **Authentication and Accounting** – Configure the authentication method for the wireless device user and enable the accounting method. The authentication and accounting configuration is optional. It only applies to Captive Portal or AAA WM-ADs.
- **RAD Policy** – Define filter ID values and WM-AD Groups. This configuration is optional.
- **Filtering** – Define filtering rules to control network access
- **Multicast** – Define groups of IP addresses for multicast traffic. This configuration is optional. By default, the multicast feature is disabled.
- **Privacy** – Select and configure the wireless security method on the WM-AD.
- **QoS Policy** – Configure the Qos Policy.

For more information, see Chapter 4, “WM Access Domain Services (WM-AD).”

Step 6 – Registering and assigning APs to the WM-AD

Deploy Altitude APs to their corresponding network locations. Connect the Altitude APs to the Summit WM series switch. Once the Altitude APs are powered on, they automatically begin the Discovery process of the Summit WM series switch, based on factors that include:

- Their Registration mode (in the **Altitude AP Registration** screen)
- The enterprise network services that will support the discovery process

A new feature available in the 4.0 release is a default AP configuration. The default AP configuration allows for a definition of a default configuration template, whereby APs automatically receive complete configuration. For typical deployments where all APs are to all have same configuration, this feature will expedite deployment, as an AP will automatically receive full configuration (including WM-AD assignment) upon initial registration with the Summit WM series switch. If applicable, modify the properties or settings of the Altitude APs.

For more information, see Chapter 5, "WM Access Domain Services configuration."

Step 7 – Confirming the AP firmware version

Confirm the latest firmware version is loaded. For more information, see "Performing Altitude AP software maintenance" on page 81.

Performing the first-time setup of the Summit WM series switch

Before you can connect the Summit WM series switch to the enterprise network, you must change the IP address of the Summit WM series switch management port from its factory default to the IP address suitable for your enterprise network. Access the Summit WM series switch by one of two methods:

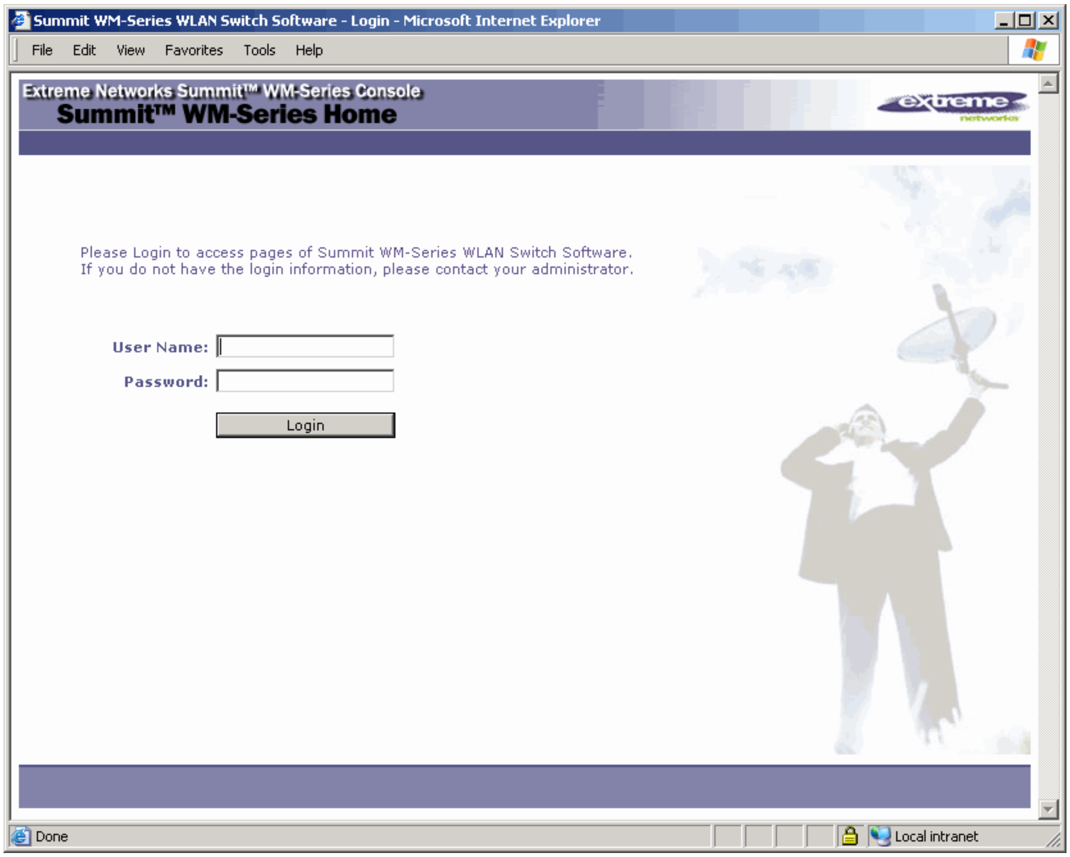
- Use a device supporting VT100 emulation, attached to the DB9 serial port (COM1 port) of the Summit WM series switch via a cross-over (null modem) cable. Use the Command Line Interface (CLI) commands. For more information, see the *Summit WM Series WLAN Switch and Altitude Access Points Software CLI Reference Guide*.
- Use a laptop computer with a Web browser. Connect the supplied cross-over Ethernet cable between the laptop and management Ethernet port of the Summit WM series switch. Follow the steps below.

Accessing the Summit WM series switch

1. Statically assign an unused IP address in the 192.168.10.0/24 subnet for the Ethernet port of the computer. For example, 192.168.10.205.
2. Launch your Web browser (Internet Explorer version 6.0 or higher, or FireFox).
3. In the browser address bar, type the following:

   ```
   https://192.168.10.1:5825
   ```

   This launches the Summit Wireless Assistant. The logon screen is displayed.


Summit WM-Series WLAN Switch Software - Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Home
extreme networks
Login
Done
Local intranet

Please Login to access pages of Summit WM-Series WLAN Switch Software.
If you do not have the login information, please contact your administrator.

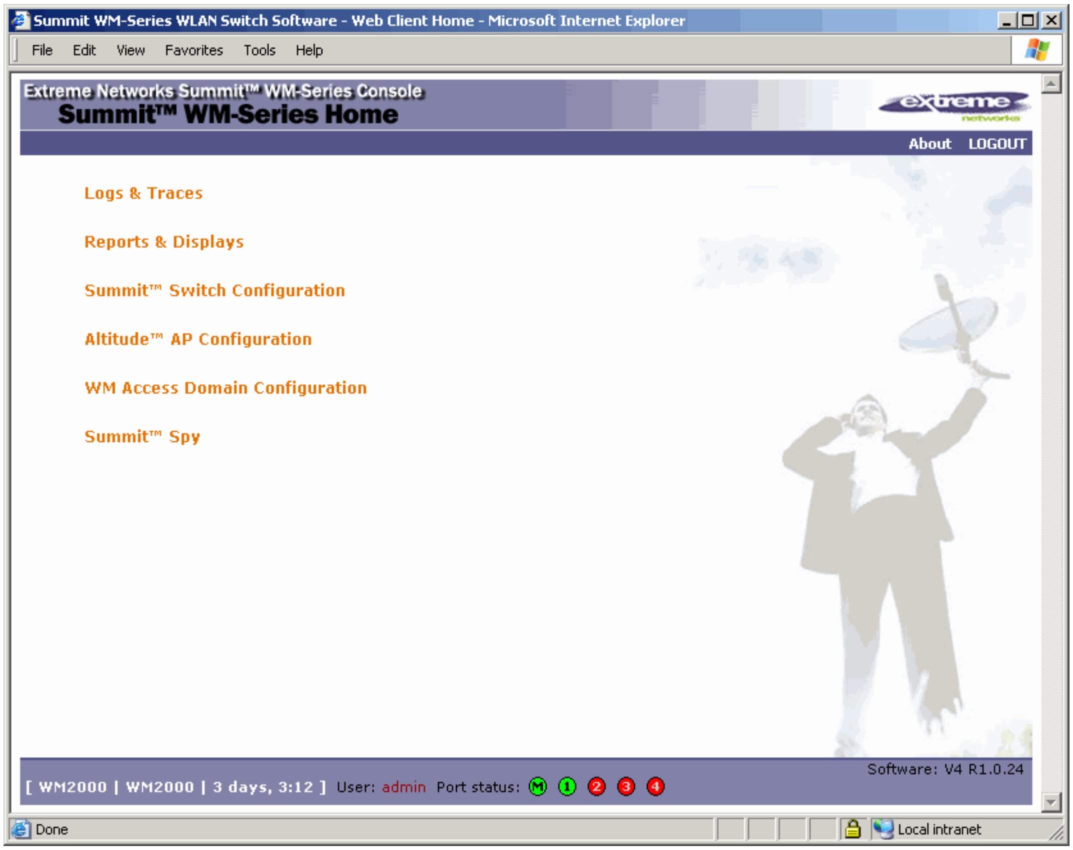
User Name:

Password:

4 In the **User Name** box, type your user name. The default is `admin`.

5 In the **Password** box, type your password. The default is `abc123`.

6 Click **Login**. The Summit Wireless Assistant main menu screen is displayed.


Summit WM-Series WLAN Switch Software - Web Client Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Home
extreme networks
About LOGOUT
Logs & Traces
Reports & Displays
Summit™ Switch Configuration
Altitude™ AP Configuration
WM Access Domain Configuration
Summit™ Spy
M
1
2
3
4
Done
Local intranet

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status:

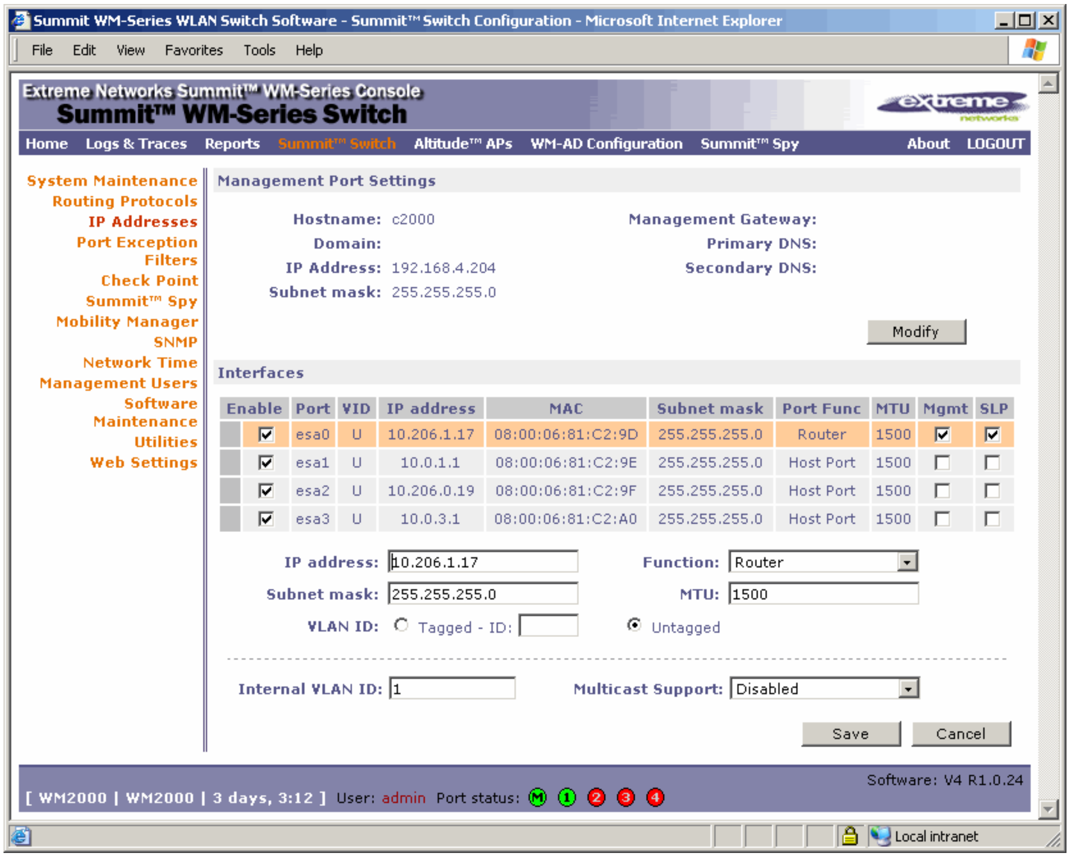
NOTE

In the footer of the Summit Wireless Assistant, the following is displayed:

- **[host name | product name | up time]**
  If there is no key (unlicensed), the product name will not be displayed.
- **User** is the user id you used to login in. For example, admin.
- **Port Status** is the connectivity state of the port. M is for the Management interface, which is on eth0 and the numbered lights reflect the esa ports on the system. Green indicates the interface is up and running. Red indicates the interface is down.

7 From the main menu, click **Summit Switch Configuration**. The **Summit WM series switch Configuration** screen is displayed.

8 In the left pane, click **IP Addresses**. The factory default settings for the Summit WM series switch are displayed.


Summit WM-Series WLAN Switch Software - Summit™ Switch Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Switch
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
System Maintenance
Routing Protocols
IP Addresses
Port Exception Filters
Check Point
Summit™ Spy
Mobility Manager
SNMP
Network Time
Management Users
Software Maintenance
Utilities
Web Settings
Modify
Save
Cancel
Local intranet

Management Port Settings

Hostname: c2000
Domain:
IP Address: 192.168.4.204
Subnet mask: 255.255.255.0
Management Gateway:
Primary DNS:
Secondary DNS:

Interfaces

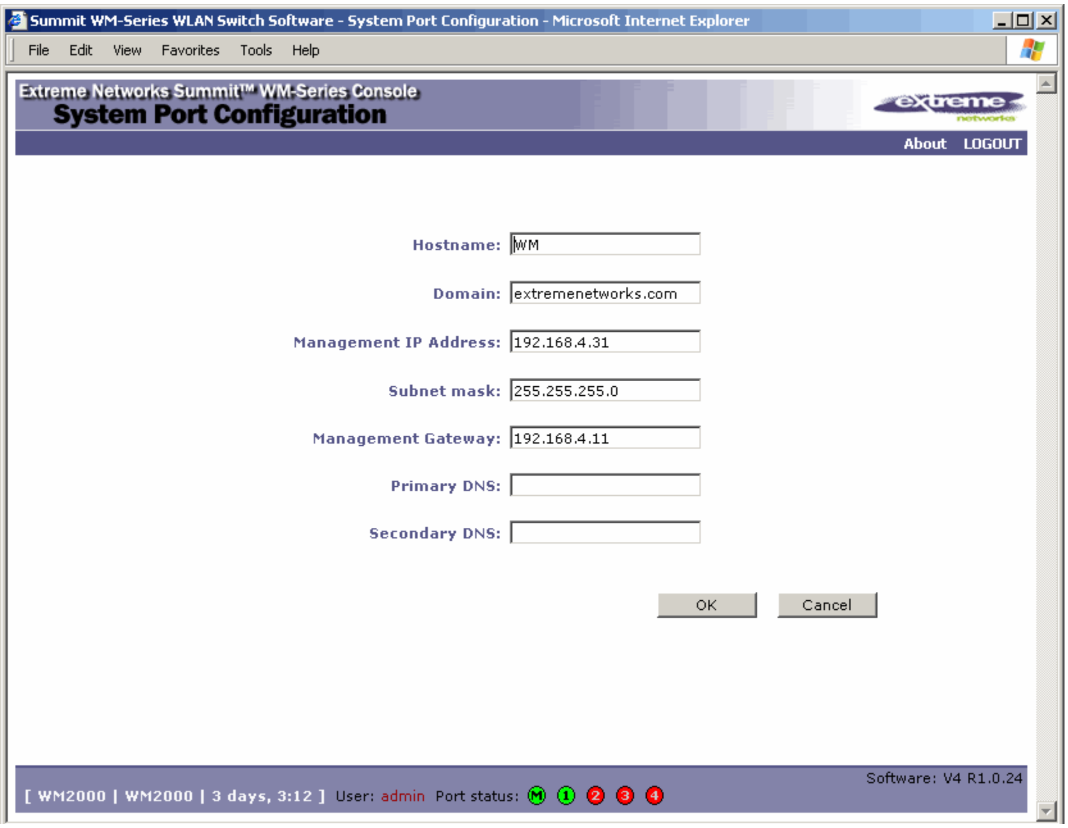
Enable	Port	VID	IP address	MAC	Subnet mask	Port Func	MTU	Mgmt	SLP
☑	esa0	U	10.206.1.17	08:00:06:81:C2:9D	255.255.255.0	Router	1500	☑	☑
☑	esa1	U	10.0.1.1	08:00:06:81:C2:9E	255.255.255.0	Host Port	1500	□	□
☑	esa2	U	10.206.0.19	08:00:06:81:C2:9F	255.255.255.0	Host Port	1500	□	□
☑	esa3	U	10.0.3.1	08:00:06:81:C2:A0	255.255.255.0	Host Port	1500	□	□

IP address: 10.206.1.17
Function: Router
Subnet mask: 255.255.255.0
MTU: 1500
VLAN ID: ○ Tagged - ID: ● Untagged

Internal VLAN ID: 1
Multicast Support: Disabled

Software: V4 R1.0.24
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

9 In the **Management Port Settings** section, click **Modify**. The **System Port Configuration** screen is displayed.


Summit WM-Series WLAN Switch Software - System Port Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
System Port Configuration
extreme networks
About LOGOUT
OK
Cancel
Software: V4 R1.0.24
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

Hostname: WM

Domain: extremenetworks.com

Management IP Address: 192.168.4.31

Subnet mask: 255.255.255.0

Management Gateway: 192.168.4.11

Primary DNS:

Secondary DNS:

10 Type the following information:

- **Hostname** – Specifies the name of the Summit WM series switch
- **Domain** – Specifies the IP domain name of the enterprise network
- **Management IP Address** – Specifies the new IP address for the Summit WM series switch’s management port. Change this as appropriate for the enterprise network.
- **Subnet mask** – Specifies the appropriate subnet mask for the IP address to separate the network portion from the host portion of the address (typically 255.255.255.0)
- **Management Gateway** – Specifies the default gateway of the network
- **Primary DNS** – Specifies the primary DNS server used by the network
- **Secondary DNS** – Specifies the secondary DNS server used by the network

11 To save your changes, click **OK.**

NOTE

The Web connection between the computer and the Summit WM series switch is now lost. The IP addresses are now set to the network you defined.

Changing the administrator password

It is recommended to change your default administrator password once your system is installed.

To change the administrator password:

1 From the main menu, click **Summit Switch Configuration**. The **Summit WM series switch Configuration** screen is displayed.

2 In the left pane, click **Management Users**.

3 In the user_admin table, click **admin**.

4 In the **Modify User Password** box, type the new administrator password.

5 In the **Modify User Confirm Password** box, type the new administrator password again.

6 Click **Change Password**.

Connecting the Summit WM series switch to your enterprise network

Once you have modified the management port configuration settings, the next step is to connect the Summit WM series switch to your enterprise network.

To connect the Summit WM series switch to your enterprise network:

1 Disconnect your computer from the Summit WM series switch management port.

2 Connect the Summit WM series switch management port to the enterprise Ethernet LAN. The Summit WM series switch resets automatically.

3 Log on to the Summit Wireless Assistant. The system is visible to the enterprise network.

Applying the product license key

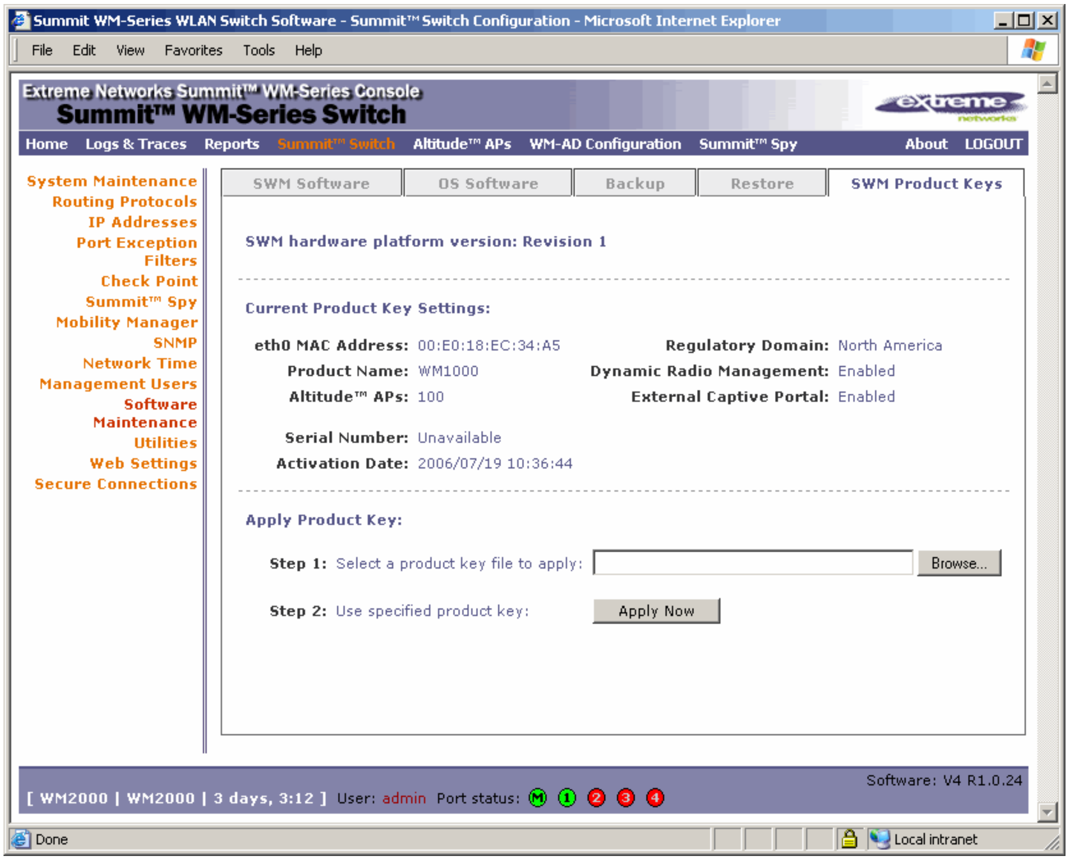
To ensure all available system functionality is enabled, your product license key must be applied.

To apply the product license key:

1 From the main menu, click **Summit Switch Configuration**. The **Summit WM series switch Configuration** screen is displayed.

2 In the left pane, click **Software Maintenance**.

3 Click the **SWM Product Keys** tab.



SWM hardware platform version: Revision 1

Current Product Key Settings:

eth0 MAC Address:	00:E0:18:EC:34:A5	Regulatory Domain:	North America
Product Name:	WM1000	Dynamic Radio Management:	Enabled
Altitude™ APs:	100	External Captive Portal:	Enabled
Serial Number:	Unavailable		
Activation Date:	2006/07/19 10:36:44		

Apply Product Key:

Step 1: Select a product key file to apply:

Step 2: Use specified product key:

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

4 In the **Apply Product Key** section, click **Browse** to navigate to the location of the product key file and select the file.

5 Click **Apply Now**. The product license key is applied.

Setting up the data ports

The next step in the initial setup of the Summit WM series switch is to configure the physical data ports.

A new Summit WM series switch is shipped from the factory with all its data ports set up as host ports. Support of management traffic is disabled on all data ports. Port configuration allows for the explicit state of the administration state for each interface. By default, data interface states will be disabled. You can then enable each of the data interfaces individually. A disabled interface does not allow data to flow (receive/transmit).

VLAN ID parameter

You can define a specific VLAN tag to be applied to a particular interface. All packets associated with that port will be tagged with the corresponding VLAN. This allows the Summit WM series switch to directly attach to a VLAN network without the need to remove VLAN tags at the connection port.

You can redefine the data ports to function as one of three types:

- Host Port

  Use a host port definition for connecting Altitude APs with no dynamic routing. A host port has dynamic routing disabled to ensure that the port does not participate in dynamic routing operations, such as OSPF, to advertise the availability of WM Access Domain Services (WM-AD) hosted by the Summit WM series switch. Host ports may still be used as the target for static route definitions.

- Third-Party AP Port

  Use a third-party AP port definition for a port to which you will connect third-party APs. Only one port can be configured for third-party APs.

  Selecting this option prepares the port to support a third-party AP setup allowing the mapping of a WM-AD to the physical port. The WM-AD settings permit the definition of policy, such as filters and Captive Portal, which manage the traffic flow for wireless users connected to these APs.

  The third-party APs must operate as layer-2 bridges. The third-party AP WM-AD is isolated from the rest of the network. The Summit WM series switch assumes control over the layer-3 functions including DHCP.

- Router Port

  Use a router port definition for a port that you want to connect to an upstream, next-hop router in the network. Dynamic routing protocol, such as OSPF, can be turned on for this port type.

  Altitude APs can be attached to a router port. The Summit WM series switch will create a virtual WM-AD port and handle wireless device traffic in the same manner as a host port.

NOTE

Third-party access points must not be directly connected to a router port.

There is a fourth port type that is not configurable in the Summit Wireless Assistant:

- WM Access Domain Services (WM-AD) interface

  A WM-AD port is a virtual port created automatically on the Summit WM series switch when a new WM-AD is defined. The WM-AD port becomes the default gateway for wireless devices on this WM-AD. No Altitude APs can be associated with a WM-AD port and no routing is permitted on this port.

The chart below summarizes the port types and their functions:

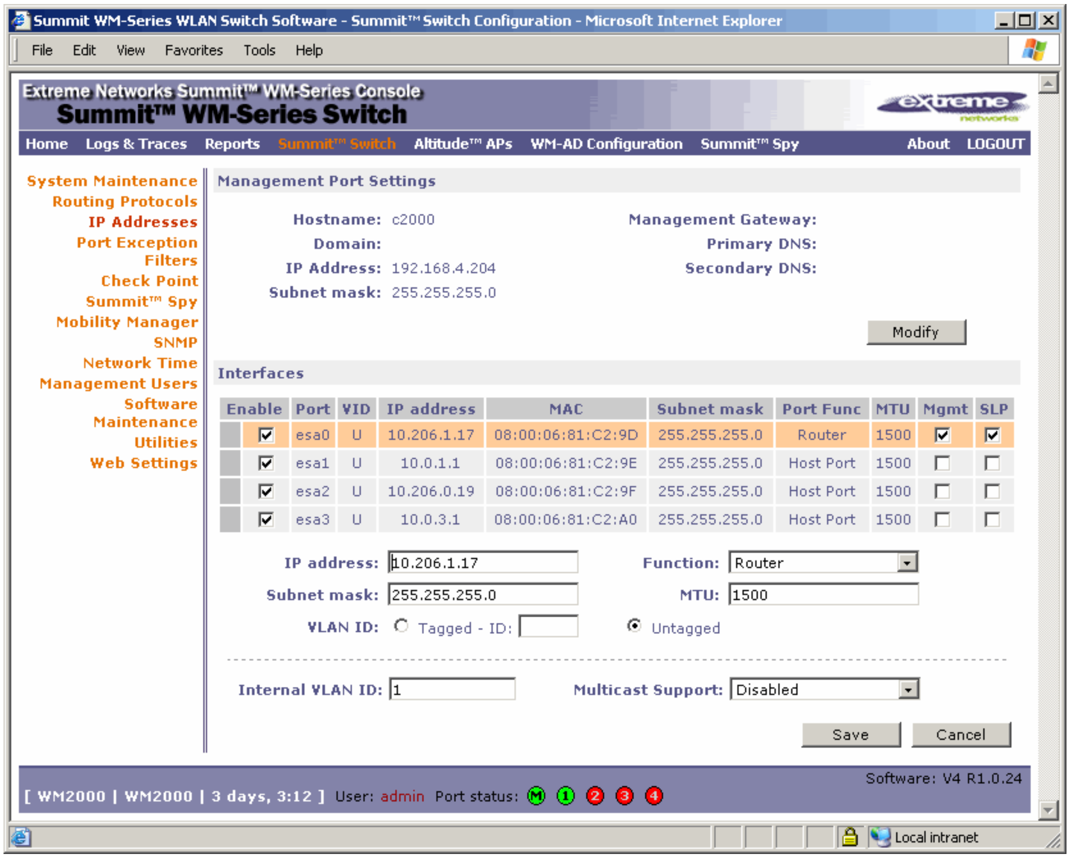
Table 2: Port types and functions

Port Type	Host	3rd-Party AP	Router	WM-AD
IP Forwarding	No	No	Selectable. Route wireless device traffic only.	No
Altitude AP support	Yes	No	Yes	No
Mgmt traffic support (SNMP, HTTP, TELNET, SLP, RADIUS, DHCP)	Selectable	Selectable	Selectable	Selectable
Routing protocol support (IP, OSPF and PIM)	No	No	Selectable	No

To configure the data port interfaces on the Summit WM series switch:

1 From the main menu, click **Summit Switch Configuration**. The **Summit WM series switch Configuration** screen is displayed.

2 In the left pane, click **IP Addresses**. The **Management Port Settings and Interfaces** screen is displayed.


Summit WM-Series WLAN Switch Software - Summit™ Switch Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Switch
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
System Maintenance
Routing Protocols
IP Addresses
Port Exception Filters
Check Point
Summit™ Spy
Mobility Manager
SNMP
Network Time
Management Users
Software Maintenance
Utilities
Web Settings
Modify
Save
Cancel
Local intranet

Management Port Settings

Hostname: c2000
Domain:
IP Address: 192.168.4.204
Subnet mask: 255.255.255.0

Management Gateway:
Primary DNS:
Secondary DNS:

Interfaces

Enable	Port	VID	IP address	MAC	Subnet mask	Port Func	MTU	Mgmt	SLP
☑	esa0	U	10.206.1.17	08:00:06:81:C2:9D	255.255.255.0	Router	1500	☑	☑
☑	esa1	U	10.0.1.1	08:00:06:81:C2:9E	255.255.255.0	Host Port	1500	□	□
☑	esa2	U	10.206.0.19	08:00:06:81:C2:9F	255.255.255.0	Host Port	1500	□	□
☑	esa3	U	10.0.3.1	08:00:06:81:C2:A0	255.255.255.0	Host Port	1500	□	□

IP address: 10.206.1.17
Subnet mask: 255.255.255.0
VLAN ID: ○ Tagged - ID: ● Untagged
Function: Router
MTU: 1500

Internal VLAN ID: 1
Multicast Support: Disabled

Software: V4 R1.0.24
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

The lower portion of the **Summit WM series switch Configuration** screen displays the four Ethernet ports. For each port, the MAC address is displayed automatically.

3 To select a port, click it.

Port configuration allows for the explicit state of the administration state for each interface. By default, data interface states will be disabled. You can then enable each of the data interfaces individually. A disabled interface does not allow data to flow (receive/transmit).

4 Type the following:

- **IP address** – The IP Address of the physical Ethernet port.
- **Subnet mask** – The appropriate subnet mask for the IP address, which separates the network portion from the host portion of the address (typically 255.255.255.0).
- **MTU** – The Maximum Transmission Unit or maximum packet size for this port. The default setting is 1500. If you change this setting and are using OSPF, be sure that the MTU of each port in the OSPF link matches.

NOTE

If the routed connection to an AP traverses a link that imposes a lower MTU than the default 1500 bytes, the Summit WM series switch and AP both participate in MTU discovery to automatically learn the correct MTU and adjust their settings accordingly. At the Summit WM series switch, MTU adjustments are tracked on a per AP basis.

5 Select a **Function** from the drop-down list:

- **Host Port** – Specifies a port for connecting Altitude APs with no dynamic routing.
- **Third-Party AP Port** – Specifies a port to which you will connect third-party access points.
- **Router Port** – Specifies a port that you want to connect to an upstream, next-hop router in the network.

NOTE

For OSPF routing on a port, the port must be configured as a router port.

6 To enable management traffic, select the **Mgmt** checkbox. Enabling management provides access to SNMP (v2, get), SSH, and HTTPs management interfaces.

NOTE

This option does not override the built-in protection filters on the port. The built-in protection filters for the port, which are restrictive in the types of packets that are allowed to reach the management plane, are extended with a set of definitions that allow for access to system management services through that interface (SSH, SNMP, HTTPS:5825).

7 To enable the SLP protocol, select the **SLP** checkbox.

Altitude APs use this port for discovery and registration. Other controllers can use this port to enable inter-controller device mobility if this port is configured to use SLP or the Summit WM series switch is running as a manager and SLP is the discovery protocol used by the agents.

8 To allow **Multicast Support**, select **Enabled** from the drop-down list.

9 To save your changes, click **Save**.

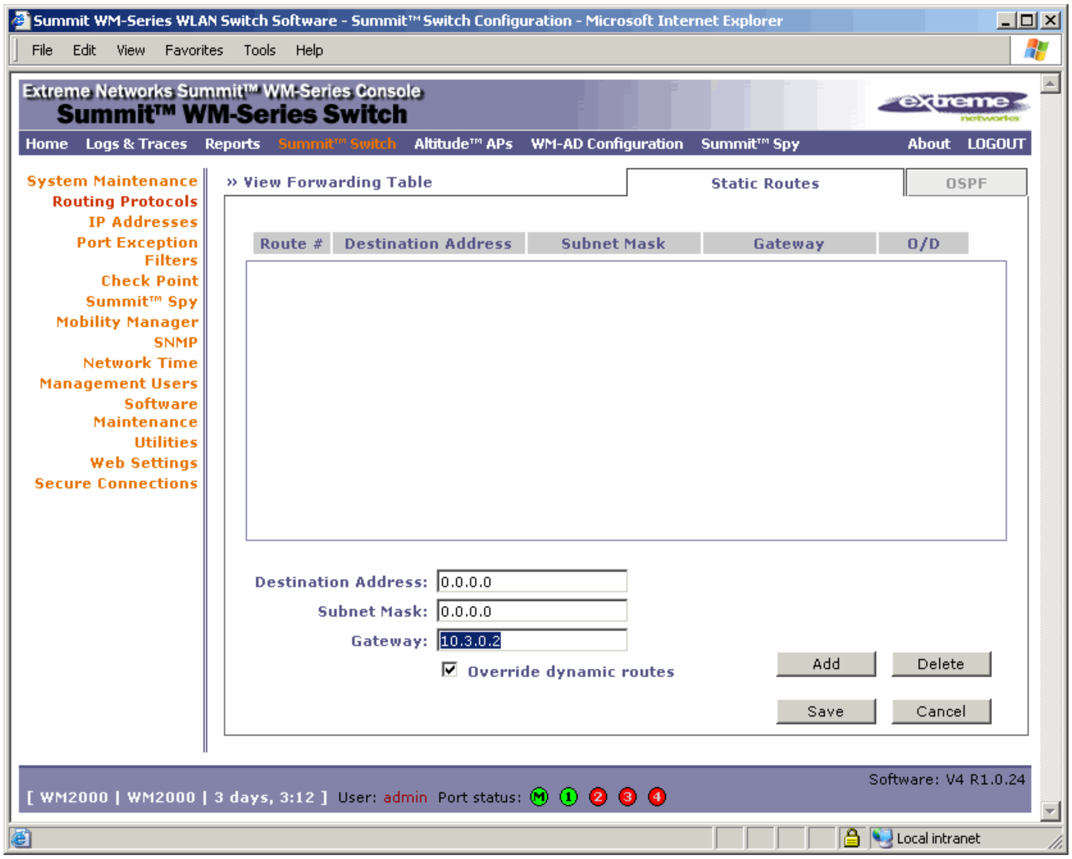
Setting up static routes

It is recommended that you define a default route to your enterprise network, either with a static route or by using OSPF protocol. A default route enables the Summit WM series switch to forward packets to destinations that do not match a more specific route definition.

To set a static route on the Summit WM series switch:

1 From the main menu, click **Summit Switch Configuration**. The **Summit WM series switch Configuration** screen is displayed.

2 In the left pane, click **Routing Protocols**. The **Static Routes** tab is displayed.



Route #	Destination Address	Subnet Mask	Gateway	O/D

Destination Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 10.3.0.2

☑ Override dynamic routes

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

3 To add a new route, in the **Destination Address** box type the destination IP address of a packet. To define a default static route for any unknown address not in the routing table, type **0.0.0.0**.

4 In the **Subnet Mask** box, type the appropriate subnet mask to separate the network portion from the host portion of the IP address (typically 255.255.255.0). To define the default static route for any unknown address, type 0.0.0.0.

5 In the **Gateway** box, type the IP address of the specific router port or gateway on the same subnet as the Summit WM series switch to which to forward these packets. This is the IP address of the next hop between the Summit WM series switch and the packet's ultimate destination.

6 Click **Add**. The new route is added to the list of routes.

7 Select the **Override dynamic routes** checkbox to give priority over the OSPF learned routes, including the default route, which the Summit WM series switch uses for routing. This option is selected by default.

To remove this priority for static routes, so that routing is controlled dynamically at all times, clear the **Override dynamic routes** checkbox.

NOTE

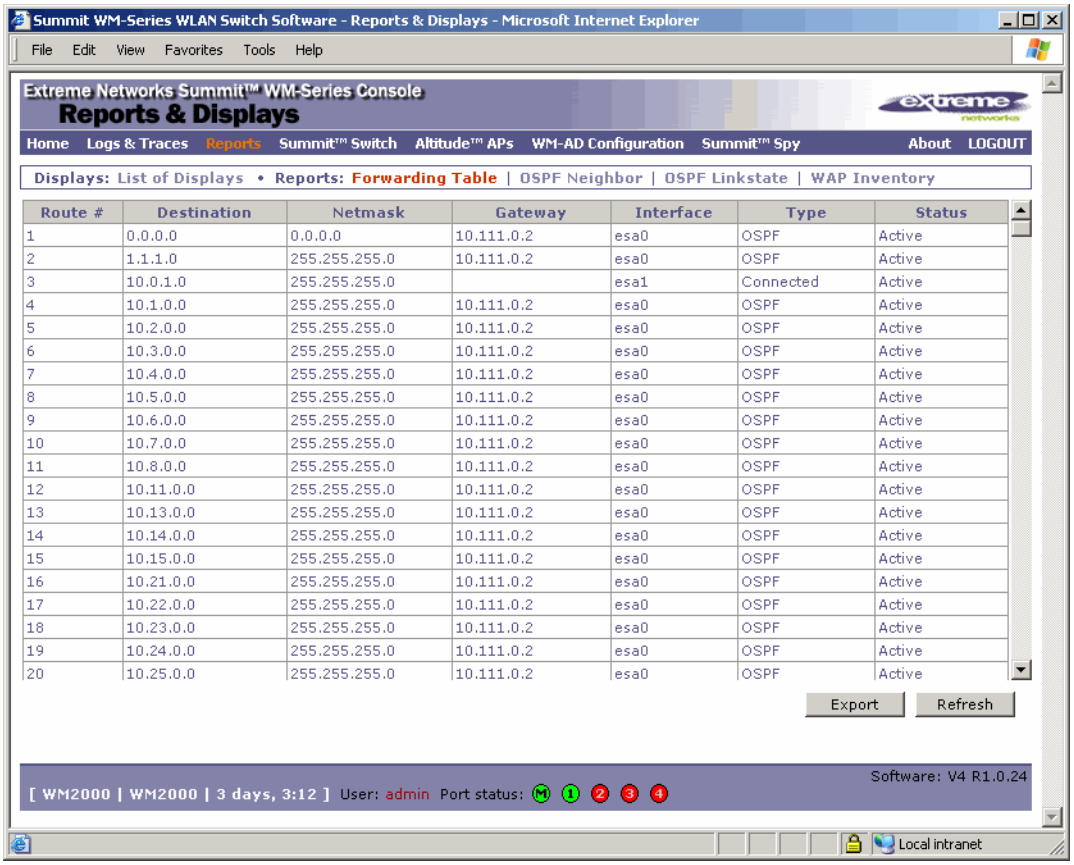
If you enable dynamic routing (OSPF), the dynamic routes will normally have priority for outgoing routing. For internal routing on the Summit WM series switch, the static routes normally have priority.

8 To save your changes, click **Save**.

To view the forwarding table on the Summit WM series switch:

1 From the main menu, click **Reports & Displays**. The **Summit Reports & Displays** screen is displayed.

2 To view the static routes that have been defined for the Summit WM series switch, click **Forwarding Table**. The **Forwarding Table** is displayed.


Summit WM-Series WLAN Switch Software - Reports & Displays - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Reports & Displays
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Displays: List of Displays • Reports: Forwarding Table | OSPF Neighbor | OSPF Linkstate | WAP Inventory

Route #	Destination	Netmask	Gateway	Interface	Type	Status
1	0.0.0.0	0.0.0.0	10.111.0.2	esa0	OSPF	Active
2	1.1.1.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
3	10.0.1.0	255.255.255.0		esa1	Connected	Active
4	10.1.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
5	10.2.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
6	10.3.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
7	10.4.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
8	10.5.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
9	10.6.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
10	10.7.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
11	10.8.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
12	10.11.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
13	10.13.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
14	10.14.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
15	10.15.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
16	10.21.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
17	10.22.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
18	10.23.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
19	10.24.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
20	10.25.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active

Export
Refresh
Software: V4 R1.0.24
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4
Local intranet

This report displays all defined routes, whether static or OSPF, and their current status.

3 To update the display, click **Refresh**.

Setting up OSPF Routing

To enable OSPF (OSPF RFC2328) routing, you must:

- Define one data port as a router port in the IP Addresses screen
- Enable OSPF globally on the Summit WM series switch
- Define the global OSPF parameters
- Enable (or disable) OSPF on the port that you defined as a router port

Ensure that the OSPF parameters defined here for the Summit WM series switch are consistent with the adjacent routers in the OSPF area. This consistency includes the following:

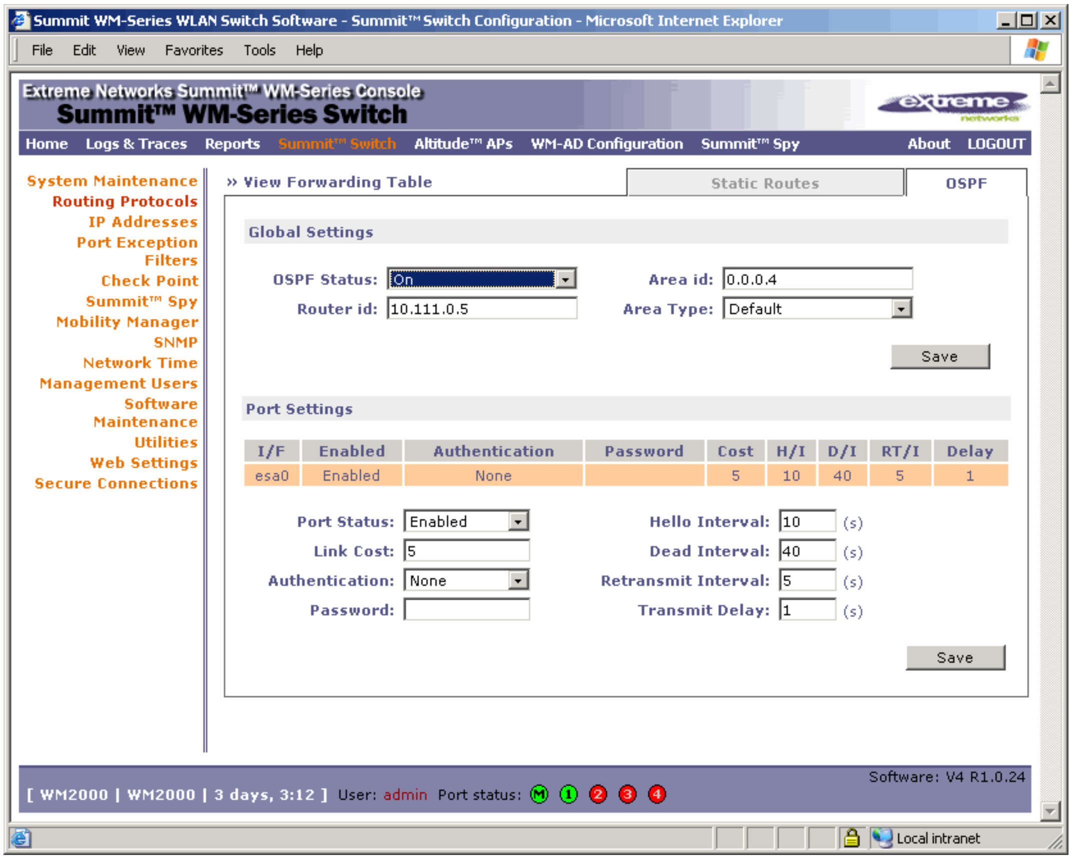
- If the peer router has different timer settings, the protocol timer settings in the Summit WM series switch must be changed to match, in order to achieve OSPF adjacency.
- The MTU of the ports on either end of an OSPF link must match. The MTU for ports on the Summit WM series switch is defined as 1500, in the **IP Addresses** screen, during data port setup. This matches the default MTU in standard routers.

To set OSPF Routing Global Settings on the Summit WM series switch:

1 From the main menu, click **Summit Switch Configuration**. The **Summit WM series switch Configuration** screen is displayed.

2 In the left pane, click **Routing Protocols**. The **Static Routes** tab is displayed.

3 Click the **OSPF** tab.



Global Settings

OSPF Status: On
Area id: 0.0.0.4
Router id: 10.111.0.5
Area Type: Default

Port Settings

I/F	Enabled	Authentication	Password	Cost	H/I	D/I	RT/I	Delay
esa0	Enabled	None		5	10	40	5	1

Port Status: Enabled
Hello Interval: 10 (s)
Link Cost: 5
Dead Interval: 40 (s)
Authentication: None
Retransmit Interval: 5 (s)
Password:
Transmit Delay: 1 (s)

Software: V4 R1.0.24
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

4 From the **OSPF Status** drop-down list, select **ON** to enable OSPF.

5 In the **Router ID** box, type the IP address of the Summit WM series switch. This ID must be unique across the OSPF area. If left blank, the OSPF daemon automatically picks a router ID from one of the Summit WM series switch's interface IP addresses.

6 In the **Area ID** box, type the area. 0.0.0.0 is the main area in OSPF.

7 From the **Area Type** drop-down list, select one of the following:

- **Default –** The default acts as the backbone area (also known as area zero). It forms the core of an OSPF network. All other areas are connected to it, and inter-area routing happens via a router connected to the backbone area.
- **Stub –** The stub area does not receive external routes. External routes are defined as routes which were distributed in OSPF via another routing protocol. Therefor, stub areas typically rely on a default route to send traffic routes outside the present domain.
- **Not-so-stubby –** The not-so-stubby area is a type of stub area that can import autonomous system (AS) external routes and send them to the default/backbone area, but cannot receive AS external routes from the backbone or other areas.

8 To save your changes, click **Save**.

To set OSPF Routing Port Settings on the Summit WM series switch:

1 From the main menu, click **Summit Switch Configuratio**n. The **Summit WM series switch Configuration** screen is displayed.

2 In the left pane, click **Routing Protocols**.

3 Click the **OSPF** tab. The **OSPF Settings** screen is displayed.

4 From the **Port Status** drop-down list, select **Enabled** to enable OSPF on the port. The default setting is **Disabled**.

5 In the **Link Cost** box, type the OSPF standard for your network for this port. This is the cost of sending a data packet on the interface. The lower the cost, the more likely the interface is to be used to forward data traffic.

NOTE

If more than one port is enabled for OSPF, it is important to prevent the Summit WM series switch from serving as a router for other network traffic (other than the traffic from wireless device users controlled by the Summit WM series switch). To ensure that the Summit WM series switch is never the preferred OSPF route, set the Link Cost to its maximum value of 65535. Filters should also be defined that will drop routed packets. For more information, see "Configuring filtering rules for a WM-AD" on page 123.

6 From the **Authentication** drop-down list, select the authentication type for OSPF on your network: **None** or **Password**. The default setting is **None**.

7 If **Password** was selected as the authentication type, in the **Password** box, type the password. If **None** was selected as the Authentication type, leave this box blank. This password must match on either end of the OSPF connection.

8 Type the following:

- **Hello-Interval –** Specifies the time in seconds (displays OSPF default). The default setting is 10 seconds.
- **Dead-Interval –** Specifies the time in seconds (displays OSPF default). The default setting is **40** seconds.
- **Retransmit-Interval –** Specifies the time in seconds (displays OSPF default). The default setting is 5 seconds.
- **Transmit Delay–** Specifies the time in seconds (displays OSPF default). The default setting is **1** second.

9 To save your changes, click **Save**.

To confirm that ports are set for OSPF:

1 To confirm that the ports are set up for OSPF, and that advertised routes from the upstream router are recognized, click **View Forwarding Table**. The **Forwarding Table** is displayed.

The following additional reports display OSPF information when the protocol is in operation:

- **OSPF Neighbor** – Displays the current neighbors for OSPF (routers that have interfaces to a common network)
- **OSPF Linkstate** – Displays the Link State Advertisements (LSAs) received by the currently running OSPF process. The LSAs describe the local state of a router or network, including the state of the router’s interfaces and adjacencies.

2 To update the display, click **Refresh**.

Filtering at the interface level

The Summit WM series switch, access points, and WLAN switch software has a number of built-in filters that protect the system from unauthorized traffic. These filters are specific only to the Summit WM series switch. These filters are applied at the network interface level and are automatically invoked. By default, these filters provide stringent-level rules to allow only access to the system's externally visible services. In addition to these built-in filters, the administrator can define specific exception filters at the interface-level to customize network access. These filters do not depend on a WM-AD definition.

Built-in port-based exception filters

On the Summit WM series switch, various port-based exception filters are built in and invoked automatically. These filters protect the Summit WM series switch from unauthorized access to system management functions and services via the ports. Access to system management functions is granted if the administrator selects the **allow management** option.

Allow management traffic is now specific to the interface being allowed. For example, if allow management is allowed on a physical port (esa0), only users connected through ESA0 will be able to get access to the system. Users connecting on any other interface such as a WM-AD (esa6) will no longer be able to target ESA0 to gain management access to the system. In order to allow access for users connected on a WM-AD, the WM-AD configuration itself must have **allow management** enabled and users will only be able to target the WM-AD interface specifically.

NOTE

You can also enable management traffic in the WM-AD definition.

For example, on the Summit WM series switch’s data interfaces (both physical interfaces and WM-AD virtual interfaces), the built-in exception filter prohibits invoking SSH, HTTPS, or SNMP. However, such traffic is allowed, by default, on the management port.

If management traffic is explicitly enabled for any interface (physical port or WM-AD), access is implicitly extended to that interface through any of the other interfaces (WM-AD). Only traffic specifically allowed by the interface’s exception filter is allowed to reach the Summit WM series switch itself. All other traffic is dropped. Exception filters are dynamically configured and regenerated whenever the system's interface topology changes (for example, a change of IP address for any interface).

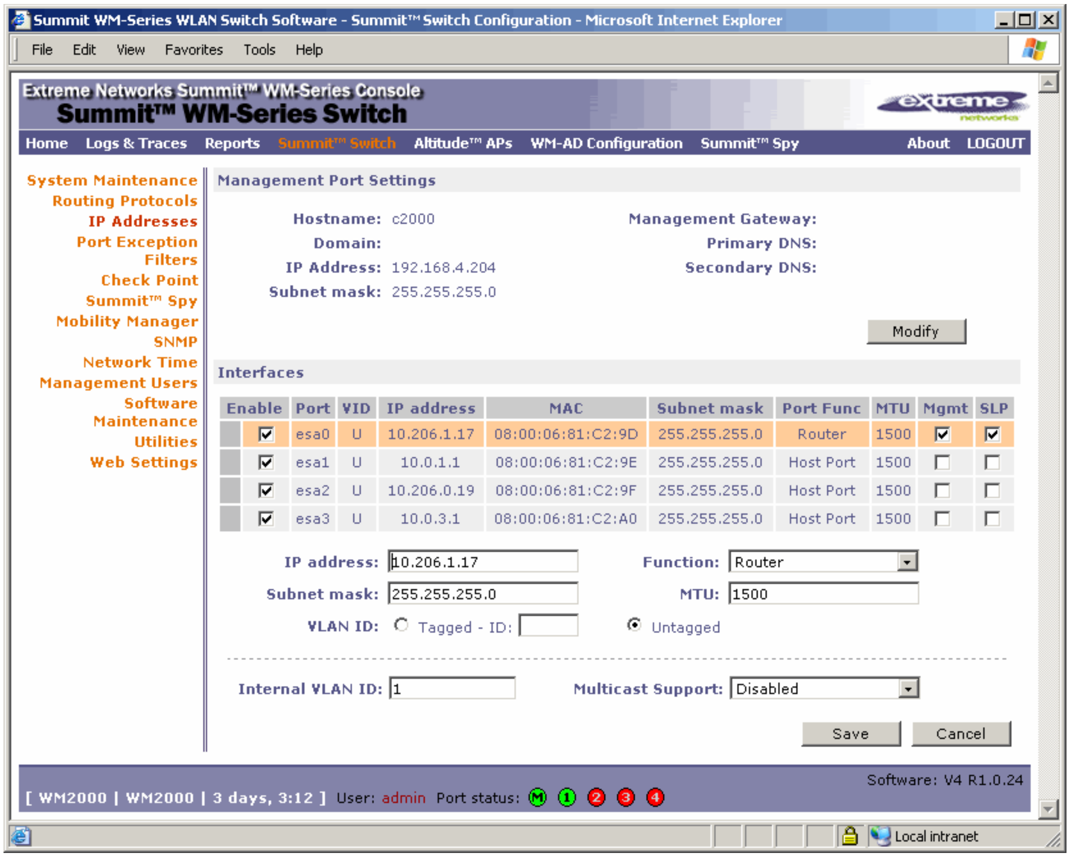
Enabling management traffic on an interface adds additional rules to the exception filter, which opens up the well-known IP(TCP/UDP) ports, corresponding to the HTTPS, SSH, and SNMP applications.

The port-based built-in exception filtering rules, in the case of traffic from WM-AD users, are applicable to traffic targeted directly for the WM-AD interface. For example, a WM-AD filter may be generic enough to allow traffic access to the Summit WM series switch's management (for example, Allow All [*.*.*.*]). Exception filter rules are evaluated after the user's WM-AD assigned filter policy, as such, it is possible that the WM-AD policy allow the access to management functions that the exception filter denies. These packets are dropped.

To enable SSH, HTTPS, or SNMP access through a data interface:

1 From the main menu, click **Summit Switch Configuration**. The **Summit WM series switch Configuration** screen is displayed.

2 In the left pane, click **IP Addresses**. The **Management Port Settings** screen is displayed.


Summit WM-Series WLAN Switch Software - Summit™ Switch Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Switch
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
System Maintenance
Routing Protocols
IP Addresses
Port Exception Filters
Check Point
Summit™ Spy
Mobility Manager
SNMP
Network Time
Management Users
Software Maintenance
Utilities
Web Settings
Modify
Save
Cancel
Local intranet

Management Port Settings

Hostname: c2000
Domain:
IP Address: 192.168.4.204
Subnet mask: 255.255.255.0
Management Gateway:
Primary DNS:
Secondary DNS:

Interfaces

Enable	Port	VID	IP address	MAC	Subnet mask	Port Func	MTU	Mgmt	SLP
☑	esa0	U	10.206.1.17	08:00:06:81:C2:9D	255.255.255.0	Router	1500	☑	☑
☑	esa1	U	10.0.1.1	08:00:06:81:C2:9E	255.255.255.0	Host Port	1500	□	□
☑	esa2	U	10.206.0.19	08:00:06:81:C2:9F	255.255.255.0	Host Port	1500	□	□
☑	esa3	U	10.0.3.1	08:00:06:81:C2:A0	255.255.255.0	Host Port	1500	□	□

IP address: 10.206.1.17
Function: Router
Subnet mask: 255.255.255.0
MTU: 1500
VLAN ID: ○ Tagged - ID: ● Untagged

Internal VLAN ID: 1
Multicast Support: Disabled

Software: V4 R1.0.24
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

3 Select the appropriate interface in the **IP Addresses** screen.

4 Select the corresponding **Management** checkbox.

5 To save your changes, click **Save**.

User defined port-based exception filters

You can add specific filtering rules at the port level in addition to the built-in rules. Such rules give you the capability of restricting access to a port, for specific reasons, such as a Denial of Service (DoS) attack.

The filtering rules are set up in the same manner as filtering rules defined for a WM-AD — specify an IP address and then either allow or deny traffic to that address. For more information, see "Configuring filtering rules for a WM-AD" on page 123.

The rules defined for port exception filters are prepended to the normal set of restrictive exception filters and have precedence over the system's normal protection enforcement.

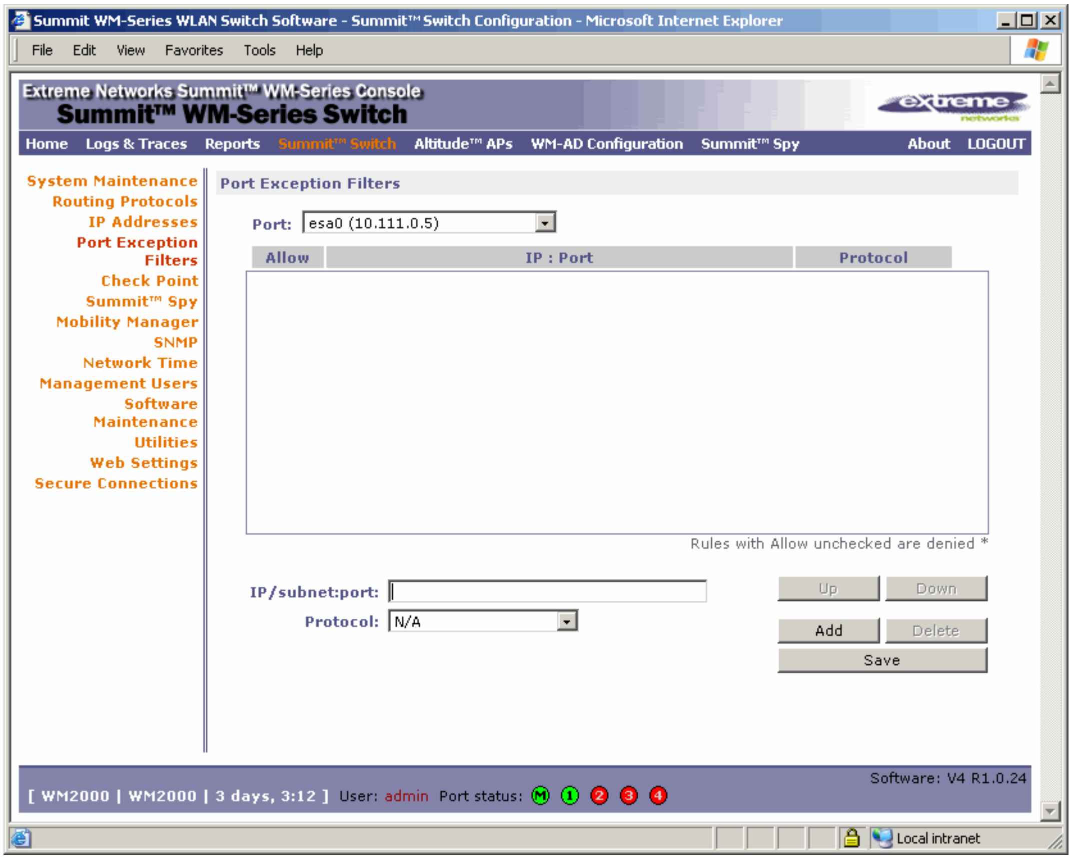
WARNING!

If defined improperly, user exception rules may seriously compromise the systems normal security enforcement rules. They may also disrupt the system's normal operation and even prevent system functionality altogether. It is advised to only augment the exception-filtering mechanism if absolutely necessary.

To define port exception filters:

1 From the main menu, click **Summit Switch Configuration**. The **Summit WM series switch Configuration** screen is displayed.

2 In the left pane, click **Port Exception Filters**. The **Port Exception Filters** screen is displayed.



Port: esa0 (10.111.0.5)

Allow	IP : Port	Protocol

Rules with Allow unchecked are denied *

IP/subnet:port:

Protocol: N/A

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

3 Select the applicable data port from the **Port** drop-down list.

4 In the **IP / subnet: port** box, type the destination IP address. You can also specify an IP range, a port designation or a port range on that IP address.

5 From the **Protocol** drop-down list, select the protocol you want to specify for the filter. This list may include **UDP**, **TCP**, **IPsec-ESP**, **IPsec-AH**, **ICMP**. The default is N/A.

6 Click **Add**. The new filter is displayed in the **Filter** section of the screen.

7 To select the new filter, click it.

8 To allow traffic, select the **Allow** checkbox.

9 To adjust the order of the filtering rules, click **Up** or **Down** to position the rule. The filtering rules are executed in the order defined here.

10 To save your changes, click **Save**.

Completing the system configuration

Once you have performed the initial configuration of the Summit WM series switch, you are now ready to do the following:

- **Configuring the WM-AD** – For more information, see Chapter 4, "WM Access Domain Services (WM-AD)."
- **Registering and assigning APs to the WM-AD** – For more information, see Chapter 3, "Configuring the Altitude AP."

Ongoing Operations of the Summit WM series switch, access points, and WLAN switch software

Once you have configured the WM-AD and registered and assigned APs to the WM-AD, the Summit WM series switch, access points, and WLAN switch software system configuration is complete. Ongoing operations of the Summit WM series switch, access points, and WLAN switch software system can include the following:

- Summit WM series switch System Maintenance
- Altitude AP Maintenance
- Client Disassociate
- Logs and Traces
- Reports and Displays

For more information, see Chapter 10, "Performing system maintenance."

3 Configuring the Altitude AP

This chapter discusses the Altitude AP and the Summit WM series switch, access points, and WLAN switch software solution, including:

- Altitude AP overview
- Discovery and registration overview
- Configuring the Altitude APs for the first time
- Adding and registering an Altitude AP manually
- Modifying Altitude AP settings
- Configuring Dynamic Radio Management
- Modifying an Altitude AP's properties based on a default AP configuration
- Modifying the Altitude AP's default setting using the Copy to Defaults feature
- Configuring APs simultaneously
- Performing Altitude AP software maintenance

Altitude AP overview

The Altitude AP is a wireless LAN access point that uses the 802.11 wireless standards (802.11a+b/g) for network communications. The Altitude AP bridges network traffic to an Ethernet LAN. The Altitude AP is provided with proprietary software that allows it to communicate only with the Summit WM series switch.

The Altitude AP physically connects to a LAN infrastructure and establishes an IP connection to the Summit WM series switch. The Altitude AP has no user interface—instead the Altitude AP is managed through the Summit Wireless Assistant. The Altitude AP's configuration is centrally managed and applied from the Summit WM series switch. In addition, the Summit WM series switch provides centralized management (verification and upgrade) of the Altitude AP firmware image.

All communication with the Summit WM series switch is carried out using a UDP-based protocol, which encapsulates IP traffic from the Altitude AP and directs it to the Summit WM series switch. The Summit WM series switch decapsulates the packets and routes them to the appropriate destinations, while managing sessions and applying policy.

Altitude AP models

The Altitude AP has two models:

- **Altitude 350-2i** – Internal antenna, internal dual (multimode) diversity antennas
- **Altitude 350-2d** – External antenna (dual external antennas), RP-SMA connectors

NOTE

In order to comply with FCC regulations in North America, the U-NII Low Band (5.15 to 5.25 GHz band) is disabled for the Model AP2620.

Altitude AP radios

The Altitude AP has two radios:

- 5 GHz radio supporting the 802.11a standard – The 802.11a standard is an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5-GHz band. The 802.11a standard uses an orthogonal frequency division multiplexing encoding scheme, rather than Frequency-Hopping Spread Spectrum (FHSS) or Direct-Sequence Spread Spectrum (DSSS).
- 2.4 GHz radio supporting the 802.11b/g standards – The 802.11g standard applies to wireless LANs and specifies a transmission rate of 54 Mbps. The 802.11b (High Rate) standard is an extension to 802.11 that specifies a transmission rate of 11 Mbps. Since 802.11g uses the same communication frequency range as 802.11b (2.4 GHz), 802.11g devices can co-exist with 802.11b devices on the same network.

The radios on the Altitude AP are enabled or disabled through the Summit Wireless Assistant. Both radios can be enabled to offer service simultaneously. For more information, see "Topology of a WM-AD" on page 87.

The Unlicensed National Information Infrastructure (U-NII) bands are three frequency bands of 100 MHz each in the 5 GHz band, designated for short-range, high-speed, wireless networking communication.

The Altitude AP supports the full range of 802.11a:

- 5.15 to 5.25 GHz – U-NII Low Band
- 5.25 to 5.35 GHz – U-NII Middle Band
- 5.725 to 5.825 GHz – U-NII High Band
- New 5.470 GHz to 5.725 GHz Band (when approved by FCC)

Altitude AP international licensing

Altitude APs are licensed to operate in North America, Japan (Altitude APs support 802.11j), the European Union countries, and European Union free trade countries. Each European Union country is assigned a particular radio band. The Altitude AP must be configured to operate on the appropriate radio band according to each European Union country. For more information, see "European Community" on page 257.

To configure the appropriate radio band according to each European Union country, use the Summit Wireless Assistant. For more information, see "Modifying an Altitude AP's properties" on page 68.

Discovery and registration overview

When the Altitude AP is powered on, it automatically begins a discovery process to determine its own IP address and the IP address of the Summit WM series switch. When the discovery process is successful, the Altitude AP registers with the Summit WM series switch.

Altitude AP discovery

Altitude APs discover the IP address of a Summit WM series switch using a sequence of mechanisms that allow for the possible services available on the enterprise network. The discovery process is successful when the Altitude AP successfully locates a Summit WM series switch to which it can register.

You must ensure that the appropriate services on your enterprise network are prepared to support the discovery process. The following five steps summarize the discovery process:

- Step 1 – Use the IP address of the last successful connection to a Summit WM series switch.

  Once an Altitude AP has successfully registered with a Summit WM series switch, it recalls that controller's IP address, and uses that address on subsequent reboots. The AP bypasses discovery and goes straight to registration. If this discovery method fails, it cycles through the remaining steps until successful.
- Step 2 – Use the predefined static IP addresses for the Summit WM series switches on the network (if configured).

  You can specify a list of static IP addresses of the Summit WM series switches on your network. On the **Static Configuration** tab, add the addresses to the **Summit Switch Search List**.

WARNING!

Altitude APs configured with a static Summit Switch Search List can only connect to Summit WM series switches in the list. Improperly configured Altitude APs cannot connect to a non-existent Summit WM series switch address, and therefore cannot receive a corrected configuration.

- Step 3 – Use Dynamic Host Configuration Protocol (DHCP) Option 78 to locate a Service Location Protocol (SLP) Directory Agent (DA), followed by a unicast SLP request to the Directory Agent.

  To use the DHCP and unicast SLP discovery method, you must ensure that the DHCP server on your network supports Option 78 (DHCP for SLP RFC2610). The Altitude APs use this method to discover the Summit WM series switch.

  This solution takes advantage of two services that are present on most networks:

  - **DHCP (Dynamic Host Configuration Protocol)** – The standard means of providing IP addresses dynamically to devices on a network.
  - **SLP (Service Location Protocol) –** A means of allowing client applications to discover network services without knowing their location beforehand. Devices advertise their services using a Service Agent (SA). In larger installations, a Directory Agent (DA) collects information from SAs and creates a central repository (SLP RFC2608).

  The Summit WM series switch contains an SLP SA that, when started, queries the DHCP server for Option 78 and if found, registers itself with the DA as service type Extreme Networks. The Summit WM series switch contains a DA (slpd).

  The Altitude AP queries DHCP servers for Option 78 in order to locate any DAs. The Altitude APs SLP User Agent then queries the DAs for a list of Extreme Networks SAs.

  Option 78 must be set for the subnets connected to the ports of the Summit WM series switch and the subnets connected to the Altitude APs. These subnets must contain an identical list of DA IP addresses.
- Step 4 – Use a Domain Name Server (DNS) lookup for the host name Controller.domain-name.

  If no DA is found, or if it has no Extreme Networks SAs registered, the Altitude AP attempts to locate a Summit WM series switch via DNS.

If you use this method for discovery, place an A record in the DNS server for Controller.<domain-name>. The <domain-name> is optional, but if used, ensure it is listed with the DHCP server.

- Step 5 – Use a multicast SLP request to find SLP SAs

  If all of the preceding methods fail to locate a Summit WM series switch, the Altitude AP sends a multicast SLP request, looking for any SLP Service Agents providing the Extreme Networks service.

Registration after discovery

Any of the discovery steps 2 through 5 can inform the Altitude AP of a list of multiple IP addresses to which the Altitude AP may attempt to connect. Once the Altitude AP has discovered these addresses, it sends out connection requests to each of them. These requests are sent simultaneously. The Altitude AP will attempt to register only with the first which responds to its request.

When the Altitude AP obtains the IP address of the Summit WM series switch, it connects and registers, sending its serial number identifier to the Summit WM series switch, and receiving from the Summit WM series switch a port IP address and binding key.

Once the Altitude AP is registered with a Summit WM series switch, the Altitude AP must be configured. After the Altitude AP is registered and configured, it can be assigned to a WM Access Domain Services (WM-AD) to handle wireless traffic.

Default Altitude AP configuration

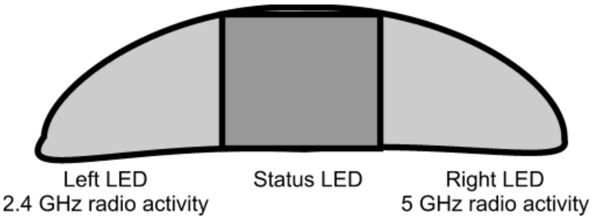
Default AP configuration simplifies the registration after discovery process. Default Altitude AP configuration acts as a configuration template that can be automatically assigned to new registering APs. The default Altitude AP configuration allows you to specify common sets of radio configuration parameters and WM-AD assignments for APs. For more information, see "Configuring the default AP settings" on page 66.

Understanding the Altitude AP LED status

When the Altitude AP is powered on and boots, you can follow its progress through the registration process by observing the LED sequence described below.

The Status LED (center) also indicates power—unlit when unit is off, and green (solid) when the AP has completed discovery and is operational.

Figure 4: Altitude AP LED



Never disconnect an Altitude AP from its power supply during a firmware upgrade.

WARNING!

Disconnecting an Altitude AP from its power supply during a firmware upgrade may cause firmware corruption rendering the AP unusable.

The table below assumes the software uses a timer and multiple phases to simulate LED blinking on all three LEDs. For example, an LED status of Red indicates the LED is solid colored Red, an LED status of Off/Green/Off indicates that the LED is Off for the first phase, Green for the second phase, and Off for the third phase.

Table 3: Altitude AP LED status

Left LED Status	Center LED Status	Right LED Status	AP Status
Off	Off	Off	Powered-off
Off	Green	Off	Beginning of Power-On-Self-Test (POST) (0.5 seconds)
Off	Off	Off	POST
Off	Red	Off	Failure during POST
Green	Off	Green	Random delay – State displayed only after a vulnerable reset
Green/Off	Off/Green	Green/Off	Vulnerable time interval – The Altitude AP resets to factory default if powered-off for three consecutive times during this state. No vulnerable period when AP is resetting to factory defaults.
Green/Off/Off	Off/Green/Off	Off/Off/Green	Resetting to factory defaults announcement – Replaces vulnerable period. This pattern is repeated twice to notify the operator when the factory configuration is restored.
Off	Orange (Green + Red)	Off	Attempting to obtain an IP address via DHCP.
Off	Red/Orange	Off	No DHCP reply has been received.
Off	Green/Orange	Off	Failed discovery (SLP).
Off	Off/Orange	Off	Summit WM series switch has been discovered. Registering the AP.
Off	Off/Red	Off	Registration of the AP has failed.
Off	Off/Green	Off	Standby, registered with a Summit WM series switch, waiting for configuration.
Green when 802.11b/g enabled Off otherwise	Green	Green when 802.11a enabled Off otherwise	Radios enabled per user settings
Off	Red/Green	Off	Upgrading firmware.

NOTE

Random delays do not occur during normal reboot. A random delay only occurs after vulnerable period power-down.

The Altitude AP can be reset to its factory default settings. For more information, see "Resetting the AP to its factory default settings" on page 207.

Configuring the Altitude APs for the first time

Before the Altitude AP is configured for the first time, you must first confirm that the following has already occurred:

- The Summit WM series switch has been set up. For more information, see Chapter 2, "Configuring the Summit WM series switch."
- The Summit WM series switch, access points, and WLAN switch software has been configured. For more information, see Chapter 2, "Configuring the Summit WM series switch."
- The Altitude APs have been installed. For more information, see the *Summit WM Series WLAN Switch Installation Instructions*.

Once the above processes are complete, you can then continue with the Altitude AP initial configuration. The Altitude AP initial configuration involves two steps:

- **Step One** – Define parameters for the discovery process. For more information, see "Defining properties for the discovery process" on page 60.
- **Step Two** – Connect the Altitude AP to a power source to initiate the discovery and registration process. For more information, see "Connecting the Altitude AP to a power source and initiating the discovery and registration process" on page 63.

Adding an Altitude AP manually option

An alternative to the automatic discovery and registration process of the Altitude AP is to manually add and register an Altitude AP to the Summit WM series switch. For more information, see "Adding and registering an Altitude AP manually" on page 63.

Defining properties for the discovery process

Before an Altitude AP is configured, you must define properties for the discovery process. The discovery process is the process by which the Altitude APs determine the IP address of the Summit WM series switch.

The properties that need to be defined are:

- Security mode
- Discovery timers

Security mode

Security mode is a Summit WM series switch property. It defines how the controller behaves when registering new, unknown devices. During the registration process, the Summit WM series switch's approval of the Altitude AP's serial number depends on the security mode that has been set:

- Allow all Altitude APs to connect
  - If the Summit WM series switch does not recognize the registering serial number, a new registration record is automatically created for the AP (if within MDL license limit). The AP receives a default configuration. The default configuration can be the default template assignment.

  - If the Summit WM series switch recognizes the serial number, it indicates that the registering device is pre-registered with the controller. The controller uses the existing registration record to authenticate the AP and the existing configuration record to configure the AP.
- Allow only approved Altitude APs to connect (this is also known as secure mode)
  - If Summit WM series switch does not recognize the AP, the AP's registration record is created in pending state (if within MDL limits). The administrator is required to manually approve a pending AP for it to provide active service. The pending AP receives minimum configuration, which only allows it to maintain an active link with the controller for future state change. The AP's radios are not configured or enabled. Pending APs are not eligible for configuration operations (WM-AD assignment, default template, Radio parameters) until approved.
  - If the Summit WM series switch recognizes the serial number, the controller uses the existing registration record to authenticate the AP. Following successful authentication, the AP is configured according to its stored configuration record.

NOTE

During the initial setup of the network, it is recommended to select the Allow all Altitude APs to connect option. This option is the most efficient way to get a large number of Altitude APs registered with the Summit WM series switch.

Once the initial setup is complete, it is recommended that the security mode is reset to the Allow only approved Altitude APs to connect option. This option ensures that no unapproved Altitude APs are allowed to connect. For more information, see "Modifying Altitude AP settings" on page 64.

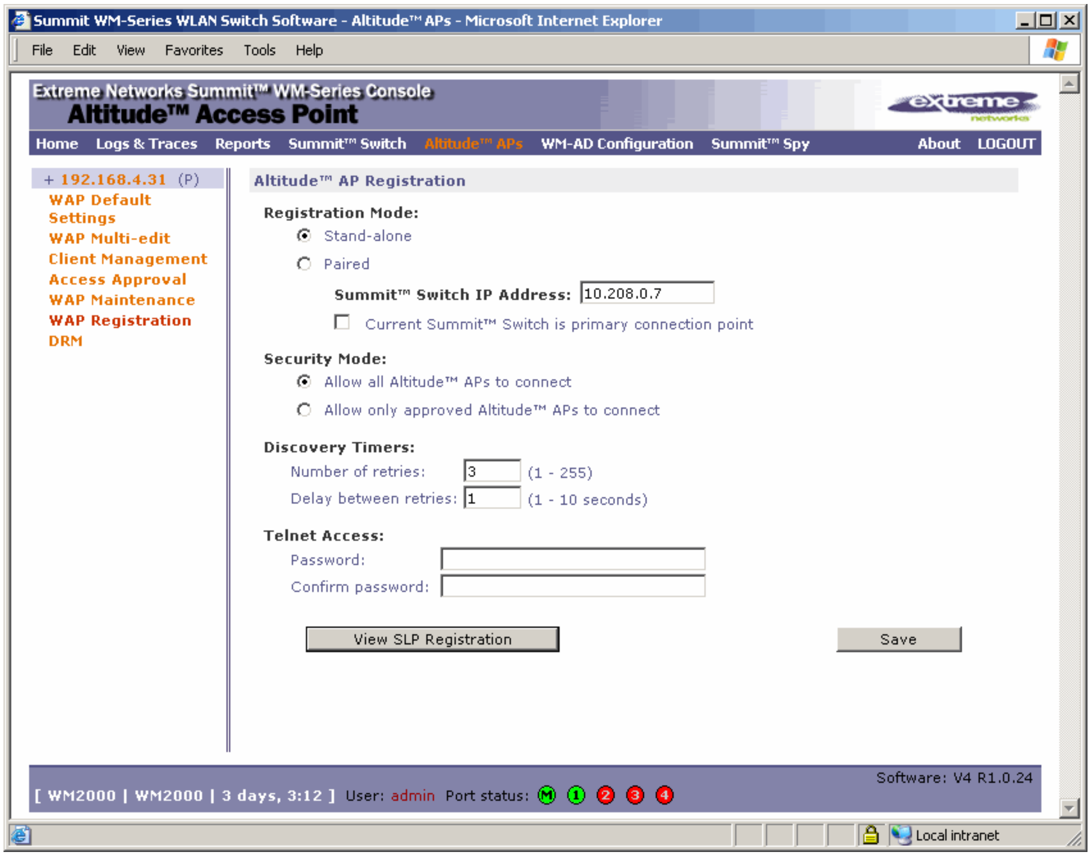
Discovery timers

The discovery timer parameters dictate the number of retry attempts and the time delay between each attempt.

To define the discovery process parameters:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP** screen is displayed.

2 In the left pane, click **WAP Registration**. The **Altitude AP Registration** screen is displayed.


Summit WM-Series WLAN Switch Software - Altitude™ APs - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Altitude™ Access Point
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
+ 192.168.4.31 (P)
WAP Default Settings
WAP Multi-edit
Client Management
Access Approval
WAP Maintenance
WAP Registration
DRM
View SLP Registration
Save
Local intranet

Altitude™ AP Registration

Registration Mode:

- ● Stand-alone
- ○ Paired

Summit™ Switch IP Address: 10.208.0.7

☐ Current Summit™ Switch is primary connection point

Security Mode:

- ● Allow all Altitude™ APs to connect
- ○ Allow only approved Altitude™ APs to connect

Discovery Timers:

Number of retries: 3 (1 - 255)

Delay between retries: 1 (1 - 10 seconds)

Telnet Access:

Password:

Confirm password:

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

3 In the Security Mode section, select one of the following:

- **Allow all Altitude APs to connect**
- Allow only approved Altitude APs to connect

The **Allow all Altitude APs to connect** option is selected by default. For more information, see "Security mode" on page 60.

4 In the Discovery Timers section, type the discovery timer values in the following boxes:

- Number of retries
- Delay between retries

The number of retries is limited to 255 in a five minutes discovery period. The default number of retries is 3, and the default delay between retries is 1 second.

5 To save your changes, click **Save**.

Once the discovery parameters are defined, you can connect the Altitude AP to a power source.

Connecting the Altitude AP to a power source and initiating the discovery and registration process

When an Altitude AP is powered on, it automatically begins the discovery and registration process with the Summit WM series switch. An Altitude AP can be connected and powered in the following ways:

- Power over Ethernet (802.3af):
  - PoE enabled switch port
  - PoE Injector
- Power by AC adaptor

For more information, see the *AP Install Guide.*

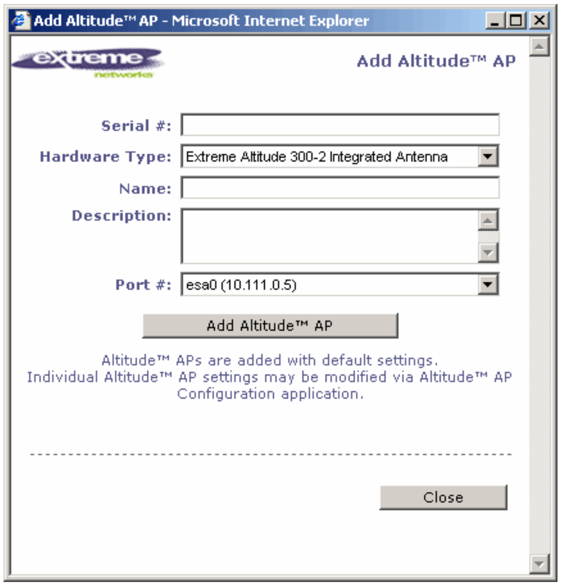
Adding and registering an Altitude AP manually

An alternative to the automatic discovery and registration process of the Altitude AP is to manually add and register an Altitude AP to the Summit WM series switch. The Altitude AP is added with default settings. For more information, see "Modifying Altitude AP settings" on page 64.

To add and register an Altitude AP manually:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP** screen is displayed.

2 Click **Add Altitude AP**. The **Add Altitude AP** screen is displayed.



Hardware Type: Extreme Altitude 300-2 Integrated Antenna

Port #: esa0 (10.111.0.5)

Altitude™ APs are added with default settings. Individual Altitude™ AP settings may be modified via Altitude™ AP Configuration application.

3 In the **Serial #** box, type the unique identifier.

4 From the **Hardware Type** drop-down list, select the hardware type of the Altitude AP.

5 In the **Name** box, type a unique name for the Altitude AP.

6 In the **Description** box, type descriptive comments for the Altitude AP.

7 In the **Port #** drop-down list, select the Ethernet port through which the Altitude AP can be reached.

8 Click **Add Altitude AP**. The Altitude AP is added and registered.

When an Altitude AP is added manually, it is added to the controller database only and does not get assigned.

9 Click **Close**.

Modifying Altitude AP settings

Altitude APs are added with default settings, which you can adjust and configure according to your network requirements. In addition, you can modify the properties and the settings for each radio on the Altitude AP.

You can also locate and select Altitude APs in specific registration states to modify their settings. For example, this feature is useful when approving pending Altitude APs when there are a large number of other Altitude APs that are already registered. From the **Access Approval** screen, click **Pending** to select all pending Altitude APs, then click **Approve** to approve all selected Altitude APs.

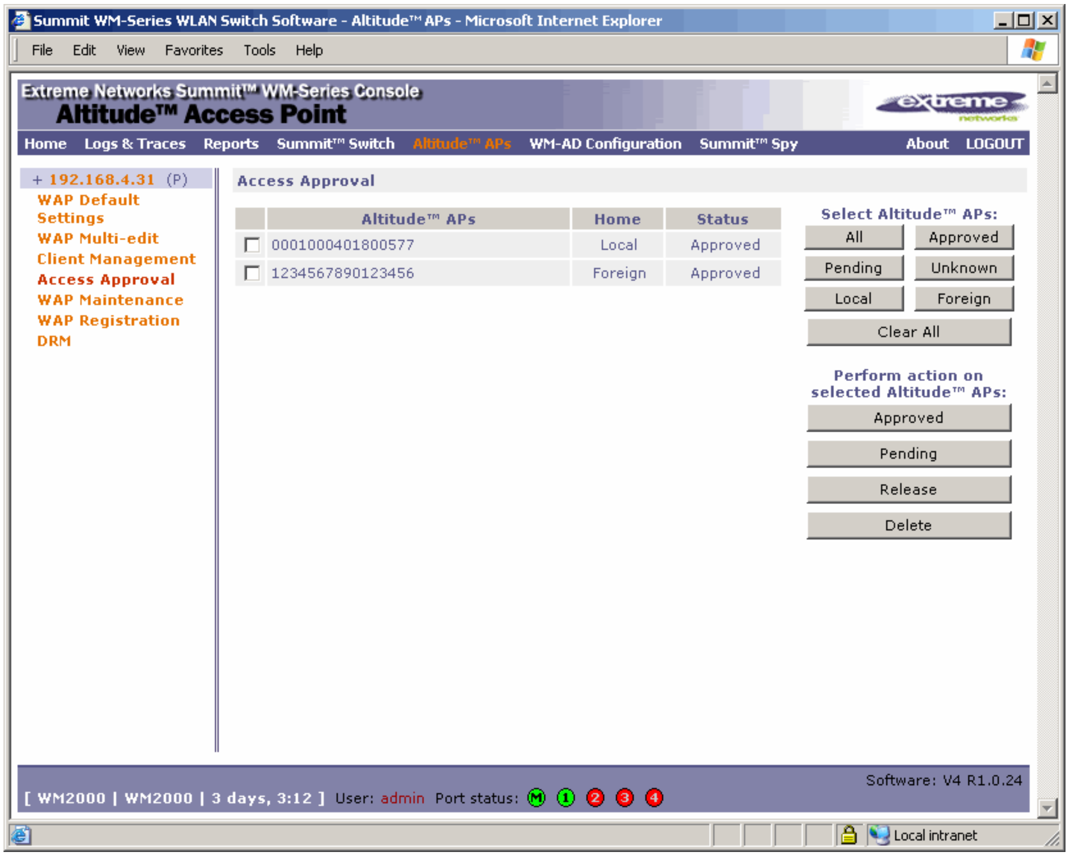
Modifying an Altitude AP's status

If during the discovery process, the Summit WM series switch security mode was **Allow only approved Altitude APs to connect**, then the status of the Altitude AP is Pending. You must modify the security mode to **Allow all Altitude APs to connect**. For more information, see "Security mode" on page 60.

To modify an Altitude AP's registration status:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP** screen is displayed.

2 In the left pane, click **Access Approval**. The **Access Approval** screen is displayed, along with the registered Altitude APs and their status.


Summit WM-Series WLAN Switch Software - Altitude™ APs - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Altitude™ Access Point
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
+ 192.168.4.31 (P)
WAP Default Settings
WAP Multi-edit
Client Management
Access Approval
WAP Maintenance
WAP Registration
DRM
Access Approval
Select Altitude™ APs:
All
Approved
Pending
Unknown
Local
Foreign
Clear All
Perform action on selected Altitude™ APs:
Approved
Pending
Release
Delete
Software: V4 R1.0.24
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4
Local intranet

	Altitude™ APs	Home	Status
☐	0001000401800577	Local	Approved
☐	1234567890123456	Foreign	Approved

3 To select the Altitude APs for status change, do one of the following:

- For a specific Altitude AP, select the corresponding checkbox.
- For Altitude APs by category, click one of the **Select Altitude APs** options.

To deselect your Altitude AP selections, click **Clear All**.

4 Click the appropriate **Perform action on selected Altitude APs** option:

- **Approved** – Change an Altitude AP's status from Pending to Approved, if the AP Registration screen was set to register only approved Altitude APs.
- **Pending** – AP is removed from the Active list, and is forced into discovery.
- **Release** – Release foreign Altitude APs after recovery from a failover. Releasing an AP corresponds to the Availability functionality. For more information, see Chapter 6, "Availability, mobility, and controller functionality."
- **Delete** – Delete this Altitude AP from the WM-AD.

Configuring the default AP settings

Altitude APs are added with default settings. You can modify the system's Altitude AP default settings accordingly, and then use these default settings to configure newly added Altitude APs. In addition, you can base the system's Altitude AP default settings on an existing Altitude AP configuration or have configured Altitude APs inherit the properties of the default Altitude AP configuration when they register with the system.

To configure the default AP settings:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP** screen is displayed.

2 In the left pane, click **AP Default Settings**.

3 Modify the following AP default settings as required:

- AP Properties
- Radio Settings
- Static Configuration
- Dynamic Radio Management
- WM-AD Assignments

4 In the AP Properties section, modify the following:

- **Poll Timeout * Interval** – Type the timeout and interval values, in seconds, for polling the controller. The default values are 10 seconds and 2 seconds, respectively.
- **Telnet Access** – Select whether Telnet Access to the Altitude AP is enabled or disabled.
- **Maintain client sessions** – Select whether the AP should remain active if a link loss with the controller occurs. This option is enabled by default.
- **Broadcast for disassoc**. – Select if you want the Altitude AP to use broadcast disassociation when disconnecting all clients, instead of disassociating each client one by one. This will affect the behavior of the AP under the following conditions:
  - If the Altitude AP is preparing to reboot or to enter one of the special modes (DRM initial channel selection).
  - If a BSSID is deactivated or removed on the Altitude AP.

  This option is enabled by default.
- **Country** – Select the country of operation. This option is only available with some licenses.

5 In the Radio Settings section, modify the following:

- **Enable Radio** – Select the radios you want to enable.
- **DTIM * Beacon Period** – For each radio, type the desired DTIM (Delivery Traffic Indication Message) period—the number of beacon intervals between two DTIM beacons. To ensure the best client power savings, use a large number. For example, 5. Use a small number for broadcast and multicast delay. The default value is **1**.
- **RTS/CTS * Frag. Threshold** – For each radio, type the packet size threshold, in bytes, above which the packet will be preceded by an RTS/CTS (Request to Send/Clear to Send) handshake. The default value is **2346**, which means all packets are sent without RTS/CTS. Reduce this value only if necessary. Also, type the fragment size threshold, in bytes, above which the packets will be fragmented by the AP prior to transmission. The default value is **2346**, which means all packets are sent unfragmented. Reduce this value only if necessary.
- **Channel** – For each radio, select the wireless channel that the Altitude AP will use to communicate with wireless devices. Depending on the regulatory domain (based on country),

some channels may be restricted. The default value is based on North America. The **Auto** selection allows the Altitude AP to select the appropriate channel automatically. For more information, see Appendix B, “Regulatory Information.”

If DRM is enabled (DRM is enabled by default), it scans automatically for a channel, using a channel selection algorithm. For more information, see “Configuring Dynamic Radio Management” on page 77.

- **TX Power Level** – For each radio, select the Tx power level: **Min**, **13%**, **25%**, **50%**, or **Max**. If Dynamic Radio Management (DRM) was enabled on the DRM screen, this option is read-only.
- **RX Diversity** – For each radio, select **Best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The default and recommended selection is **Best**. If only one antenna is connected, use the corresponding **Left** or **Right** diversity setting. Do not use **Best** if two identical antennas are not used.
- **TX Diversity** – For each radio, select **Best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The default selection is **Best**, which maximizes performance for most clients. However, some clients may behave oddly with Tx Diversity set to **Best**. Under those circumstances, it is recommended to use either Left or Right for Tx Diversity. If only one antenna is connected, use the corresponding **Left** or **Right** diversity setting. Do not use **Best** if two identical antennas are not used.
- **Operational Rate Set** – For each radio, select the data rate that clients can operate at while associated with the AP: **1**, **2**, **5.5**, **6**, **9**, **11**, **12**, **18**, **24**, **36**, **48**, or **54** Mbps. The **Best data rate** allows the Altitude AP to select the best data rate automatically.
- **Basic Rates** – Select the data rates that must be supported by all stations in a BSS: **1**, **2** or **1**, **2**, **5.5**, and **11** Mbps.
- **Preamble** – Select a preamble type for 11b-specific (CCK) rates: **Short**, **Long**, or **Auto**. The recommended value is **Auto**. Select **Short** if you are sure that there is no pre-11b AP or a client in the vicinity of this AP. Select **Long** if compatibility with pre-11b clients is required.
- **Protection Mode** – Select a protection mode: **None**, **Auto**, or **Always**. The default and recommended setting is **Auto**. Select **None** if 11b APs and clients are not expected. Select **Always** if you expect many 11b-only clients.
- **Protection Rate** – Select a protection rate: **1**, **2**, **5.5**, or **11** Mbps. The default and recommended setting is **11**. Only reduce the rate if there are many 11b clients in the environment or if the deployment has areas with poor coverage. For example, rates lower than **11** Mbps are required to ensure coverage.
- **Protection Type** – Select a protection type: **CTS Only** or **RTS CTS**. The default and recommended setting is **CTS Only**. Select **RTS CTS** only if an 11b AP that operates on the same channel is detected in the neighborhood, or if there are many 11b-only clients in the environment.
- **Min Basic Rate** – For both radios, select the minimum data rate that must be supported by all stations in a BSS: **1**, **2**, **5.5**, or **11** Mbps for 11b and 11b+11g modes. Select **1**, **2**, **5.5**, **6**, **11**, **12**, or **24** Mbps for 11g-only mode. If necessary, the **Max Basic Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**. If both **Min Basic Rate** and **Max Basic Rate** are set to an 11g-specific (OFDM) rate, (for example, **6**, **12**, or **24** Mbps) all basic rates will be 11g-specific.
- **Max Basic Rate** – For both radios, Select the maximum data rate that must be supported by all stations in a BSS: **1**, **2**, **5.5**, or **11** Mbps for 11b and 11b+11g modes. Select **1**, **2**, **5.5**, **6**, **11**, **12**, or **24** Mbps for 11g-only mode. If necessary, the **Max Basic Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**. If both **Min Basic Rate** and **Max Basic Rate** are set to an 11g-specific (OFDM) rate, (for example, **6**, **12**, or **24** Mbps) all basic rates will be 11g-specific.
- **Max Operational Rate** – Select the maximum data rate that clients can operate at while associated with the AP: **1**, **2**, **5.5**, or **11** Mbps for 11b-only mode. Select **1**, **2**, **5.5**, **6**, **9**, **11**, **12**, **18**, **24**,

36, **28**, or **54** Mbps for 11b+11g or 11g-only modes. If necessary, the **Max Operational Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**.

6 In the **Static Configuration** section, modify the following:

- In the **Add** box, type the IP address of the Summit WM series switch that will control this Altitude AP.
- Click **Add**. The IP address is added to the list.
- Repeat to add additional Summit WM series switches.
- Click **Up** and **Down** to modify the order of the controllers. The maximum is three controllers.

  The Altitude AP attempts to connect to the IP addresses in the order in which they are listed. The Altitude AP is successful when it finds a Summit WM series switch that will allow it to register.

  This feature allows the Altitude AP to bypass the discovery process. If the **Summit Switch Search List** box is not populated, the Altitude AP will use SLP to discover a Summit WM series switch.

  The DHCP function for wireless clients must be provided locally by a local DHCP server, unless each wireless client has a static IP address.

7 In the **Dynamic Radio Management** section, modify the following:

- **Enable** – Select **Enable** or **Disable**. DRM is enabled by default.
- **Coverage** – Select **Shaped** or **Standard**. Shaped coverage adjusts the range based on neighboring Altitude APs and standard coverage adjusts the range to the client that is the most distant, as indicated by its signal strength.
- **Avoid WLAN** – For each radio, select **On** or **Off.**
- **Minimum TX** – For each radio, select the minimum power level that the range of transmit power can be adjusted dynamically.
- **Maximum TX** – For each radio, select the maximum power level that the range of transmit power can be adjusted dynamically.

8 In the **WM-AD Assignments** section, assign the radios for each WM-AD in the list by selecting or clearing the radio checkboxes.

9 To save your changes, click **Save**.

Modifying an Altitude AP’s properties

Once an Altitude AP has successfully registered, you can then modify its properties. Modifying an AP’s properties can include modifying properties on the following tabs:

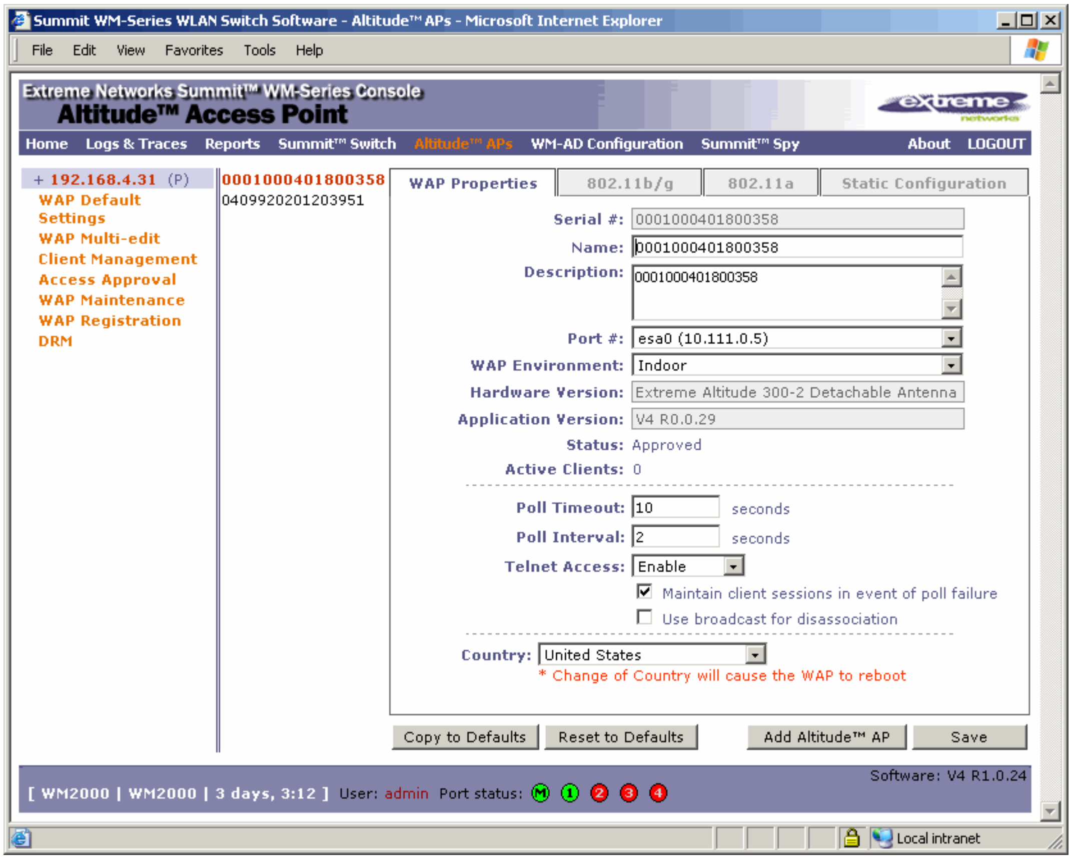
- AP properties
- 802.11b/g
- 802.11a
- Static Configuration

Modifying an AP’s properties is similar to modifying the system’s default AP settings, only now you are modifying an individual Altitude AP.

To modify an Altitude AP's properties:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP** screen is displayed.

2 In the **Altitude AP** list, click the Altitude AP whose properties you want to modify. The **AP Properties** tab displays Altitude AP information.



Serial #: 0001000401800358

Name: 0001000401800358

Description: 0001000401800358

Port #: esa0 (10.111.0.5)

WAP Environment: Indoor

Hardware Version: Extreme Altitude 300-2 Detachable Antenna

Application Version: V4 R0.0.29

Status: Approved

Active Clients: 0

Poll Timeout: 10 seconds

Poll Interval: 2 seconds

Telnet Access: Enable

☑ Maintain client sessions in event of poll failure

☐ Use broadcast for disassociation

Country: United States

* Change of Country will cause the WAP to reboot

3 Modify the Altitude AP's information:

- **Name** – Type a unique name for the Altitude AP that identifies the AP. The default value is the Altitude AP's serial number.
- **Description** – Type comments for the Altitude AP.
- **Port #** – Select the Ethernet port of the switch the Altitude AP is connected to.
- **Poll Timeout** – Type the timeout value, in seconds, for polling the controller. The default value is 10 seconds.
- **Poll Interval** – Type the interval value, in seconds, for polling the controller. The default value is 2 seconds.
- **Telnet Access** – Select whether Telnet Access to the Altitude AP is enabled or disabled.
- **Maintain client session in event of poll failure –** Select this option if the AP should remain active if a link loss with the controller occurs.This option is enabled by default.
- **Use broadcast for disassociation –** Select if you want the Altitude AP to use broadcast disassociation when disconnecting all clients, instead of disassociating each client one by one. This will affect the behavior of the AP under the following conditions:
  - If the Altitude AP is preparing to reboot or to enter one of the special modes (DRM initial channel selection).

- ■ If a BSSID is deactivated or removed on the Altitude AP.

  This option is disabled by default.
- **Country –** Select the country of operation. This option is only available with some licenses.

The following on the **AP Properties** tab are view only:

- **Serial # –** Displays a unique identifier that is assigned during the manufacturing process.
- **Hardware Version –** Displays the current version of the Altitude AP hardware.
- **Application Version –** Displays the current version of the Altitude AP software.
- **Status**:

  Approved – Indicates that the Altitude AP has received its binding key from the Summit WM series switch after the discovery process.

  ■ **Pending –** Indicates that the Altitude AP has not yet successfully been approved for access with the secure controller.

  You can modify the status of an Altitude AP on the Access Approval screen. For more information, see "Modifying an Altitude AP's status" on page 64.
- **Active Clients –** Displays the number of wireless devices currently active on the Altitude AP.

4 To save your changes, click **Save**.

Modifying the Altitude AP's radio properties

Most properties of the Altitude AP's radios can be modified without requiring a reboot of the Altitude AP. However, modifying the following will require a reboot of the Altitude AP:

- Enabling or disabling either radio
- Changing the radio channel between Auto and any fixed channel number

If the Altitude AP does require a reboot, a warning message is displayed to the user in the Summit Wireless Assistant.

To modify the Altitude AP's radio properties:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP** screen is displayed.

2 Click the appropriate Altitude AP in the list.

3 Click the radio tab you want to modify.

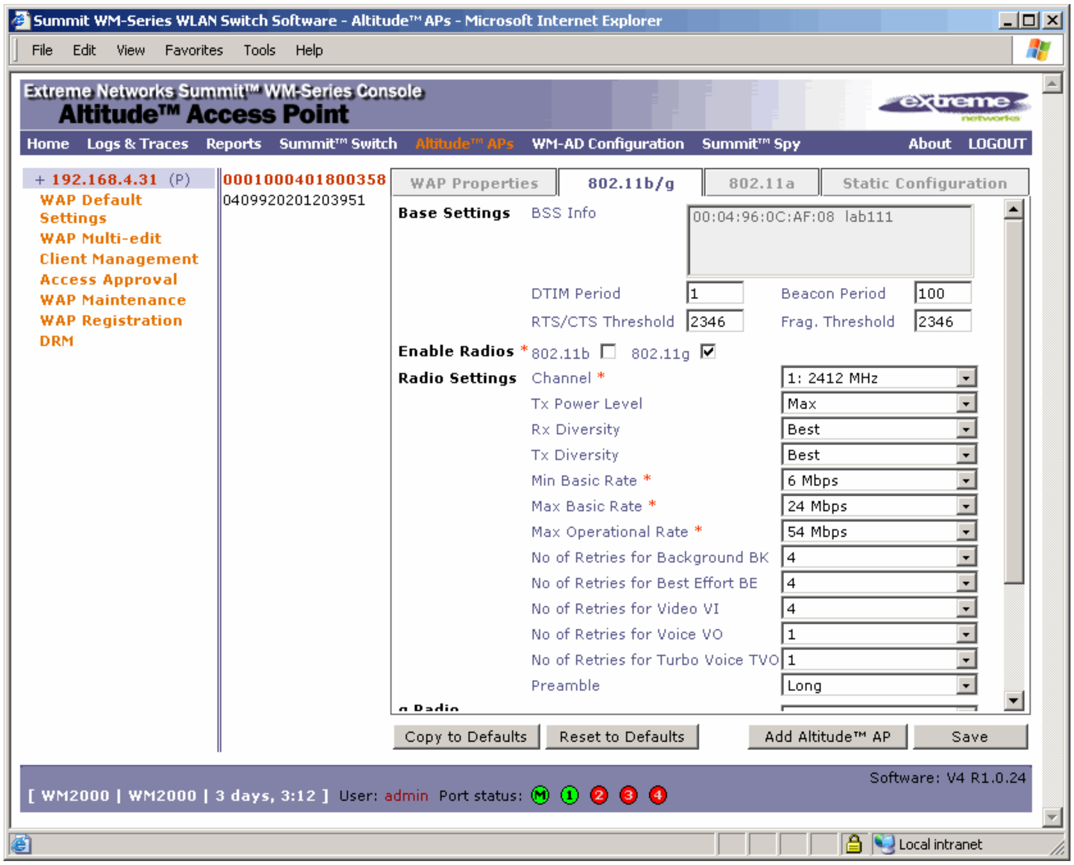
Each tab displays the radio settings for each radio on the Altitude AP. If the radio has been assigned to a WM-AD, the WM-AD names and MAC addresses appear in the **Base Settings** section. The following lists the number of WM-ADs that each Summit WM series switch can support:

- WM200 -- up to 32 WM-ADs
- WM2000 -- up to 64 WM-ADs

The AP radios can be assigned to each of the configured WM-ADs in a system. Each AP can be the subject of 8 WM-AD assignments (corresponding to the number of SSIDs it can support). Once a radio has all 8 slots assigned, it is no longer eligible for further assignment.

The **BSS Info** section is view only. After WM-AD configuration, the **Basic Service Set (BSS)** section displays the MAC address on the Altitude AP for each WM-AD and the SSIDs of the WM-ADs to which this radio has been assigned.

- If applicable, click the **802.11b/g** tab to modify the radio properties.



Summit WM-Series WLAN Switch Software - Altitude™ APs - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Altitude™ Access Point
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
+ 192.168.4.31 (P)
WAP Default Settings
WAP Multi-edit
Client Management
Access Approval
WAP Maintenance
WAP Registration
DRM
WAP Properties
802.11b/g
802.11a
Static Configuration
Copy to Defaults
Reset to Defaults
Add Altitude™ AP
Save
Local intranet

0001000401800358
0409920201203951

Base Settings

BSS Info: 00:04:96:0C:AF:08 lab111

DTIM Period: 1 | Beacon Period: 100

RTS/CTS Threshold: 2346 | Frag. Threshold: 2346

Enable Radios * 802.11b □ 802.11g ☑

Radio Settings

Channel *: 1: 2412 MHz

Tx Power Level: Max

Rx Diversity: Best

Tx Diversity: Best

Min Basic Rate *: 6 Mbps

Max Basic Rate *: 24 Mbps

Max Operational Rate *: 54 Mbps

No of Retries for Background BK: 4

No of Retries for Best Effort BE: 4

No of Retries for Video VI: 4

No of Retries for Voice VO: 1

No of Retries for Turbo Voice TVO: 1

Preamble: Long

g Radio

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

- **DTIM Period** – Type the desired DTIM (Delivery Traffic Indication Message) period—the number of beacon intervals between two DTIM beacons. To ensure the best client power savings, use a large number. For example, 5. Use a small number for broadcast and multicast delay. The default value is **1**.
- **Beacon Period** – Type the desired time, in milliseconds, between beacon transmissions. The default value is **100** milliseconds.
- **RTS/CTS Threshold** – Type the packet size threshold, in bytes, above which the packet will be preceded by an RTS/CTS (Request to Send/Clear to Send) handshake. The default value is **2346**, which means all packets are sent without RTS/CTS. Reduce this value only if necessary.
- **Frag. Threshold** – Type the fragment size threshold, in bytes, above which the packets will be fragmented by the AP prior to transmission. The default value is **2346**, which means all packets are sent unfragmented. Reduce this value only if necessary.
- **802.11b** – Select to enable the 802.11b mode of the 802.11b/g radio. If disabled, the AP will not accept associations from 11b clients.
- **802.11g** – Select to enable the 802.11g mode of the 802.11b/g radio. If disabled, the AP will use 11g-specific (OFDM) rates with all of the associated clients.
- **Channel** – Select the wireless channel that the Altitude AP will use to communicate with wireless devices. Depending on the regulatory domain (based on country), some channels may be restricted. The default value is based on North America. The **Auto** selection allows the Altitude AP to select the appropriate channel automatically. For more information, see Appendix B, “Regulatory Information.”

If DRM is enabled (DRM is enabled by default), it scans automatically for a channel, using a channel selection algorithm. For more information, see "Configuring Dynamic Radio Management" on page 77.

- **Tx Power Level –** Select the Tx power level: **Min**, **13%**, **25%**, **50%**, or **Max**. If Dynamic Radio Management (DRM) was enabled on the DRM screen, this option is read-only.
- **Rx Diversity –** Select **Best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The default and recommended selection is **Best**. If only one antennae is connected, use the corresponding **Left** or **Right** diversity setting. Do not use **Best** if two identical antennas are not used.
- **Tx Diversity –** Select **Best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The default selection is **Best**, which maximizes performance for most clients. However, some clients may behave oddly with Tx Diversity set to **Best**. Under those circumstances, it is recommended to use either Left or Right for Tx Diversity. If only one antennae is connected, use the corresponding **Left** or **Right** diversity setting. Do not use **Best** if two identical antennas are not used.
- **Min Basic Rate –** Select the minimum data rate that must be supported by all stations in a BSS: **1**, **2**, **5.5**, or **11** Mbps for 11b and 11b+11g modes. Select **1**, **2**, **5.5**, **6**, **11**, **12**, or **24** Mbps for 11g-only mode. If necessary, the **Max Basic Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**. If both **Min Basic Rate** and **Max Basic Rate** are set to an 11g-specific (OFDM) rate, (for example, **6**, **12**, or **24** Mbps) all basic rates will be 11g-specific.
- **Max Basic Rate –** Select the maximum data rate that must be supported by all stations in a BSS: **1**, **2**, **5.5**, or **11** Mbps for 11b and 11b+11g modes. Select **1**, **2**, **5.5**, **6**, **11**, **12**, or **24** Mbps for 11g-only mode. If necessary, the **Max Basic Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**. If both **Min Basic Rate** and **Max Basic Rate** are set to an 11g-specific (OFDM) rate, (for example, **6**, **12**, or **24** Mbps) all basic rates will be 11g-specific.
- **Max Operational Rate –** Select the maximum data rate that clients can operate at while associated with the AP: **1**, **2**, **5.5**, or **11** Mbps for 11b-only mode. Select **1**, **2**, **5.5**, **6**, **9**, **11**, **12**, **18**, **24**, **36**, **28**, or **54** Mbps for 11b+11g or 11g-only modes. If necessary, the **Max Operational Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**.
- **No of Retries for Background BK –** Select the number of retries for the Background transmission queue. The default value is **4**. The recommended setting is **adaptive (multi-rate)**.
- **No of Retries for Best Effort BE –** Select the number of retries for the Best Effort transmission queue. The default value is **4**. The recommended setting is **adaptive (multi-rate)**.
- **No of Retries for Video VI –** Select the number of retries for the Video transmission queue. The default value is **4**. The recommended setting is **adaptive (multi-rate)**.
- **No of Retries for Voice VO –** Select the number of retries for the Voice transmission queue. The default value is **1**. The recommended setting is **adaptive (multi-rate)**.
- **No of Retries for Turbo Voice TVO –** Select the number of retries for the Turbo Voice transmission queue. The default value is **1**. The recommended setting is **adaptive (multi-rate)**.
- **Preamble –** Select a preamble type for 11b-specific (CCK) rates: **Short**, **Long**, or **Auto**. The recommended value is **Auto**. Select **Short** if you are sure that there is no pre-11b AP or a client in the vicinity of this AP. Select **Long** if compatibility with pre-11b clients is required.
- **Protection Mode –** Select a protection mode: **None**, **Auto**, or **Always**. The default and recommended setting is **Auto**. Select **None** if 11b APs and clients are not expected. Select **Always** if you expect many 11b-only clients.
- **Protection Rate –** Select a protection rate: **1**, **2**, **5.5**, or **11** Mbps. The default and recommended setting is **11**. Only reduce the rate if there are many 11b clients in the environment or if the deployment has areas with poor coverage. For example, rates lower than **11** Mbps are required to ensure coverage.

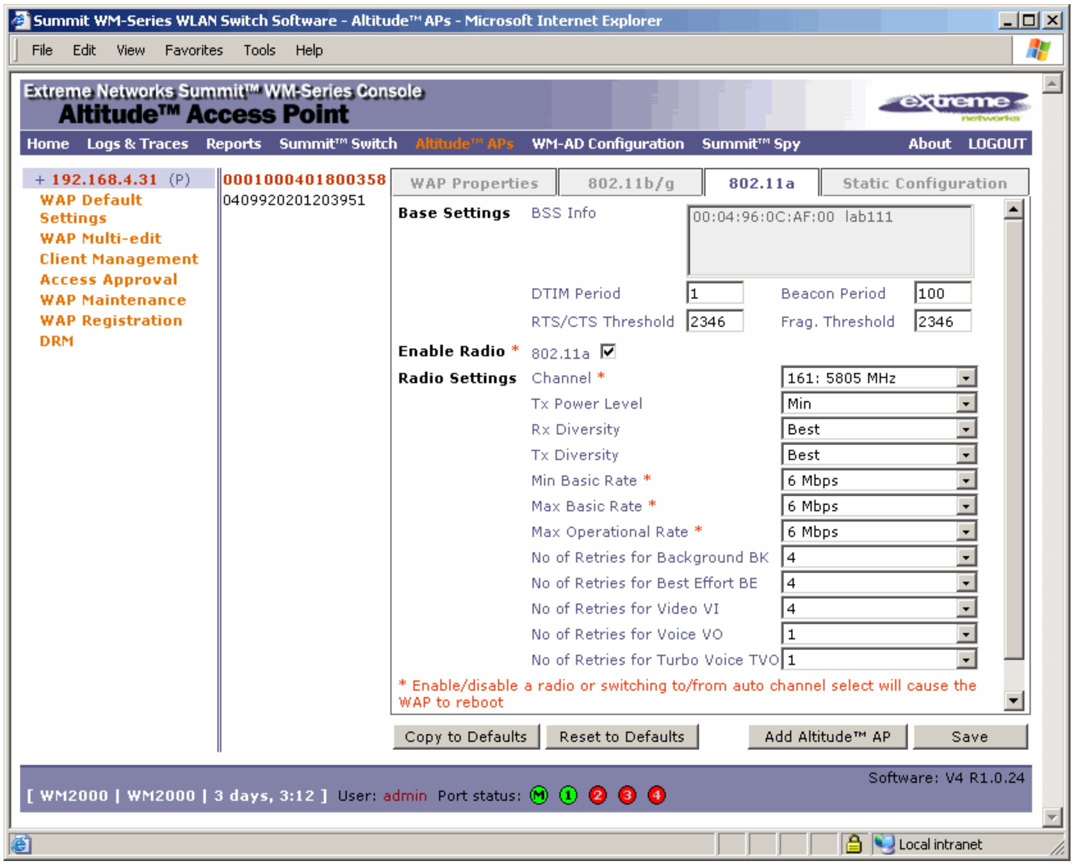
- **Protection Type –** Select a protection type: **CTS Only** or **RTS CTS**. The default and recommended setting is **CTS Only**. Select **RTS CTS** only if an 11b AP that operates on the same channel is detected in the neighborhood, or if there are many 11b-only clients in the environment.

NOTE

The overall throughput is reduced when Protection Mode is enabled, due to the additional overhead caused by the RTS/CTS. The overhead is minimized by setting Protection Type to CTS Only and Protection Rate to 11 Mbps. Although, the overhead causes the overall throughput to be sometimes lower than if just 11b mode is used. If there are many 11b clients, it is recommended to disable 11g support (11g clients are backward compatible with 11b APs).

An alternate approach, although a more expensive method, is to dedicate all APs on a channel for 11b (for example, disable 11g on these APs) and disable 11b on all other APs. The difficulty with this method is that the number of APs must be increased to ensure coverage separately for 11b and 11g clients.

- If applicable, click the **802.11a** tab to modify the radio properties.



Base Settings

BSS Info: 00:04:96:0C:AF:00 lab111

DTIM Period: 1

Beacon Period: 100

RTS/CTS Threshold: 2346

Frag. Threshold: 2346

Enable Radio * 802.11a ☑

Radio Settings

Channel *: 161: 5805 MHz

Tx Power Level: Min

Rx Diversity: Best

Tx Diversity: Best

Min Basic Rate *: 6 Mbps

Max Basic Rate *: 6 Mbps

Max Operational Rate *: 6 Mbps

No of Retries for Background BK: 4

No of Retries for Best Effort BE: 4

No of Retries for Video VI: 4

No of Retries for Voice VO: 1

No of Retries for Turbo Voice TVO: 1

* Enable/disable a radio or switching to/from auto channel select will cause the WAP to reboot

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

- **DTIM Period –** Type the desired DTIM (Delivery Traffic Indication Message) period—the number of beacon intervals between two DTIM beacons. To ensure the best client power savings, use a large number. For example, 5. Use a small number for broadcast and multicast delay. The default value is **1**.
- **Beacon Period –** Type the desired time, in milliseconds, between beacon transmissions. The default value is **100** milliseconds.

- **RTS/CTS Threshold** – Type the packet size threshold, in bytes, above which the packet will be preceded by an RTS/CTS (Request to Send/Clear to Send) handshake. The default value is **2346**, which means all packets are sent without RTS/CTS. Reduce this value only if necessary.
- **Frag. Threshold** – Type the fragment size threshold, in bytes, above which the packets will be fragmented by the AP prior to transmission. The default value is **2346**, which means all packets are sent unfragmented. Reduce this value only if necessary.
- **802.11a** – Select to enable the 802.11a radio.
- **802.11j** – Select to enable the 802.11j mode for the 802.11a radio. This option is available only in Japan. When enabled, it allows access to the 4.9Ghz and 5.0Ghz wireless bands.
- **Channel** – Select the wireless channel that the Altitude AP will use to communicate with wireless devices. Depending on the regulatory domain (based on country), some channels may be restricted. The default value is based on North America. The **Auto** selection allows the Altitude AP to select the appropriate channel automatically. For more information, see Appendix B, "Regulatory Information."

  If DRM is enabled (DRM is enabled by default), it scans automatically for a channel, using a channel selection algorithm. For more information, see "Configuring Dynamic Radio Management" on page 77.
- **Tx Power Level** – Select the Tx power level: **Min**, **13%**, **25%**, **50%**, or **Max**. If Dynamic Radio Management (DRM) was enabled on the DRM screen, this option is read-only.
- **Rx Diversity** – Select **Best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The default and recommended selection is **Best**. If only one antennae is connected, use the corresponding **Left** or **Right** diversity setting. Do not use **Best** if two identical antennas are not used.
- **Tx Diversity** – Select **Best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The default selection is **Best**, which maximizes performance for most clients. However, some clients may behave oddly with Tx Diversity set to **Best**. Under those circumstances, it is recommended to use either Left or Right for Tx Diversity. If only one antennae is connected, use the corresponding **Left** or **Right** diversity setting. Do not use **Best** if two identical antennas are not used.
- **Min Basic Rate** – Select the minimum data rate that must be supported by all stations in a BSS: **6**, **12**, or **24** Mbps. If necessary, the **Max Basic Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**.
- **Max Basic Rate** – Select the maximum data rate that must be supported by all stations in a BSS: **6**, **12**, or **24** Mbps. If necessary, the **Max Basic Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**.
- **Max Operational Rate** – Select the maximum data rate that clients can operate at while associated with the AP: **6**, **9**, **12**, **18**, **24**, **36**, **48**, or **54** Mbps. If necessary, the **Max Operational Rate** choices adjust automatically to be higher or equal to the **Max Basic Rate**.

NOTE

Radio a channels 100 to 140 occupy the 5470-5725 MHz band in the regulatory domains of the European Union and European Union free trade countries. Radio B/G Channels 12 to 14 are not available in North America.

- **No of Retries for Background BK** – Select the number of retries for the Background transmission queue. The default value is **4**. The recommended setting is **adaptive (multi-rate)**.
- **No of Retries for Best Effort BE** – Select the number of retries for the Best Effort transmission queue. The default value is **4**. The recommended setting is **adaptive (multi-rate)**.

- **No of Retries for Video VI** – Select the number of retries for the Video transmission queue. The default value is **4**. The recommended setting is **adaptive (multi-rate)**.
- **No of Retries for Voice VO** – Select the number of retries for the Voice transmission queue. The default value is **1**. The recommended setting is **adaptive (multi-rate)**.
- **No of Retries for Turbo Voice TVO** – Select the number of retries for the Turbo Voice transmission queue. The default value is **1**. The recommended setting is **adaptive (multi-rate)**.

4 To save your changes, click **Save.**

Setting up the Altitude AP using static configuration

The Altitude AP static configuration feature provides the Summit WM series switch, access points, and WLAN switch software solution with the capability for a network with either a central office or a branch office model. The static configuration settings assist in the setup of branch office support. These settings are not dependent of branch topology, but instead can be employed at any time if required. In the branch office model, Altitude APs are installed in remote sites, while the Summit WM series switch is in the central office. The Altitude APs require the capability to interact in both the local site network and the central network. To achieve this model, a static configuration is used.

NOTE

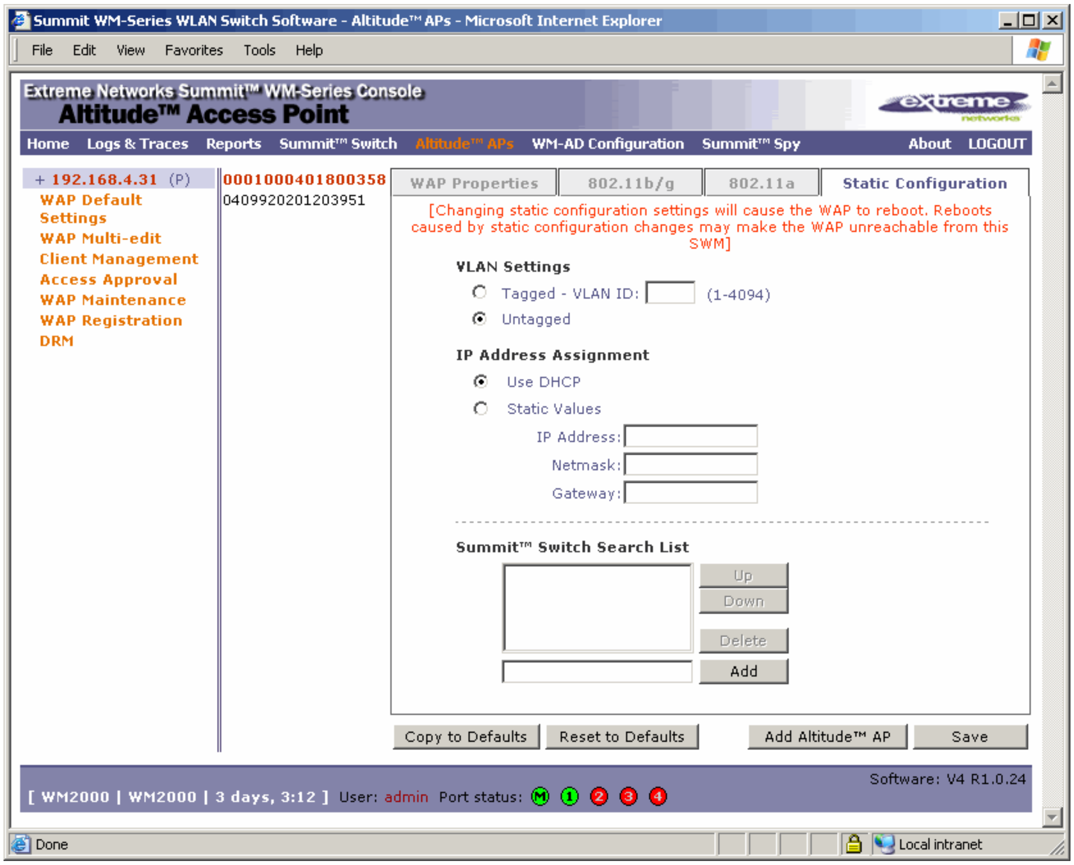
If an Altitude AP with a statically configured IP address (without a statically configured Summit Switch Search List) cannot register with the Summit WM series switch within the specified number of retries, the Altitude AP will use SLP, DNS, and SLP multicast as a backup mechanism.

To set up an Altitude AP using static configuration:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP** screen is displayed.

2 Click the appropriate Altitude AP in the list.

3 Click the **Static Configuration** tab.



[Changing static configuration settings will cause the WAP to reboot. Reboots caused by static configuration changes may make the WAP unreachable from this SWM]

VLAN Settings

○ Tagged - VLAN ID: (1-4094)

● Untagged

IP Address Assignment

● Use DHCP

○ Static Values

IP Address:

Netmask:

Gateway:

Summit™ Switch Search List

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

4 Select one of the VLAN settings for the Altitude AP:

- **Tagged - VLAN ID –** Select if you want to assign this AP to a specific VLAN and type the value in the box.
- **Untagged –** Select if you want this AP to be untagged. This option is selected by default.

WARNING!

Caution should be exercised when using this feature. If a VLAN tag is not configured properly, the connectivity with the AP will be lost. To configure the AP VLAN, do the following:

Connect the AP to the Summit WM series switch or to the network point that does not require AP VLAN tagging.

Use Static Configuration to enable VLAN and define the VLAN ID.

Save the configuration on the AP. The AP reboots and looses connectivity to the Summit WM series switch.

Disconnect the AP and attach it to its final network location.

If the VLAN settings match the network configuration, the AP registers with the Summit WM series switch successfully. If the AP VLAN is not configured properly (wrong tag), connecting to the AP may not be possible. To recover from this situation, you will need to reset the AP to its factory default settings. For more information, see "Resetting the AP to its factory default settings" on page 207.

5 Select one of the two methods of IP address assignment for the Altitude AP:

- **Use DHCP –** Select this option to enable Dynamic Host Configuration Protocol (DHCP). This option is enabled by default.
- **Static Values –** Select this option to specify the IP address of the Altitude AP.
  - **IP Address –** Type the IP address of the AP.
  - **Subnet Mask –** Type the appropriate subnet mask to separate the network portion from the host portion of the address.
  - **Gateway –** Type the default gateway of the network.

NOTE

For first-time deployment of the Altitude AP for static IP assignment, (a branch office scenario is an example of a setup that may require static IP assignment), it is recommended to use DHCP initially on the central office network to obtain an IP address for the Altitude AP. Then enter these values in the Static Configuration tab for this Altitude AP and save the configuration. Since APs ship from the factory with DHCP mode enabled by default, the APs require the assistance of a local DHCP server to obtain its initial IP address. The AP can then register with the controller, at which point it can receive the proper static definition parameters and be moved to its target location if necessary.

If the AP IP address is not configured properly, connecting to the AP may not be possible. To recover from this situation, you will need to reset the AP to its factory default settings. For more information, see "Resetting the AP to its factory default settings" on page 207.

6 In the **Add** box, type the IP address of the Summit WM series switch that will control this Altitude AP.

7 Click **Add**. The IP address is added to the list.

8 Repeat steps 5 and 6 to add additional Summit WM series switches.

9 Use the **Up** and **Down** buttons to modify the order of the controllers. The maximum is three controllers.

The Altitude AP attempts to connect to the IP addresses in the order in which they are listed. The Altitude AP is successful when it finds a Summit WM series switch that will allow it to register.

This feature allows the Altitude AP to bypass the discovery process. If the **Summit Switch Search List** box is not populated, the Altitude AP will use SLP to discover a Summit WM series switch.

The DHCP function for wireless clients must be provided locally by a local DHCP server, unless each wireless client has a static IP address.

10 To save your changes, click **Save**.

Configuring Dynamic Radio Management

The Dynamic Radio Management (DRM) feature for the Altitude AP is enabled by default. The DRM feature:

- Adjusts power levels to balance coverage if another Altitude AP, which is assigned to the same SSID and is on the same channel, is added to or leaves the network.
- Allows wireless clients to be moved to another Altitude AP if the load is too high.
- Scans automatically for a channel, using a channel selection algorithm.

- Avoids other WLANs by reducing transmit power whenever other APs with the same channel, but different SSIDs are detected.

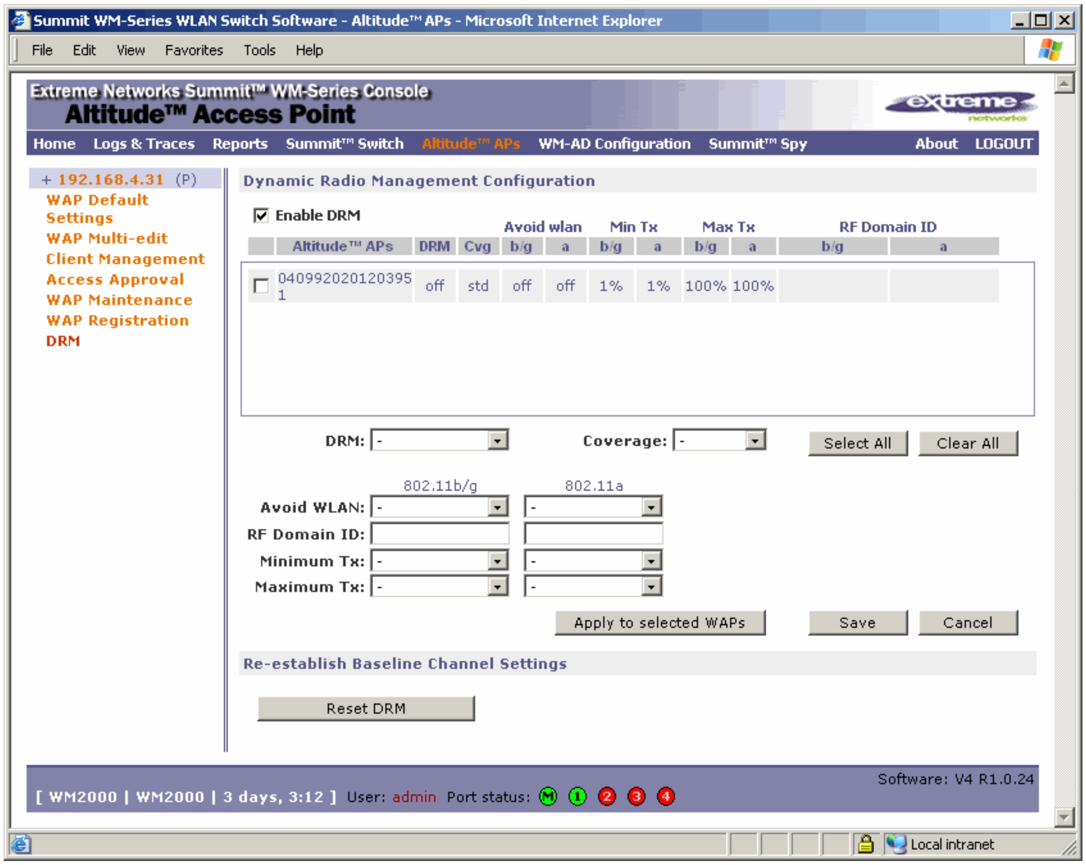
To configure the DRM software:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP** screen is displayed.

2 In the left pane, click **DRM**.

3 Confirm the **Enable DRM** checkbox is selected.

4 To refresh the **Altitude APs** list, click **Save**. The list is populated with the Altitude APs.


Summit WM-Series WLAN Switch Software - Altitude™ APs - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Altitude™ Access Point
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
+ 192.168.4.31 (P)
WAP Default Settings
WAP Multi-edit
Client Management
Access Approval
WAP Maintenance
WAP Registration
DRM
Select All
Clear All
Apply to selected WAPs
Save
Cancel
Reset DRM
Local intranet

Dynamic Radio Management Configuration

☑ Enable DRM

	Altitude™ APs	DRM	Cvg	Avoid wlan b/g	Avoid wlan a	Min Tx b/g	Min Tx a	Max Tx b/g	Max Tx a	RF Domain ID b/g	RF Domain ID a
☐	0409920201203951	off	std	off	off	1%	1%	100%	100%		

DRM: - Coverage: -

	802.11b/g	802.11a
Avoid WLAN:	-	-
RF Domain ID:		
Minimum Tx:	-	-
Maximum Tx:	-	-

Re-establish Baseline Channel Settings

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

5 From the list of registered Altitude APs, select the checkbox corresponding to the Altitude AP you want to configure for DRM. The DRM properties are populated with default values when DRM is enabled.

6 In the **Coverage** drop-down list, select:

- **Std** – (Standard Coverage) Adjusts the range to the client that is the most distant, as indicated by its signal strength.
- **Shpd** – (Shaped Coverage) Adjusts the range based on neighboring Altitude APs.

7 If applicable, from the **Avoid WLAN** drop-down list, select **on.**

8 In the **RF Domain ID** box, type a string that uniquely identifies a group of APs that cooperate in managing RF channels and power levels. The maximum length of the string is 15 characters.

NOTE

If SSID Broadcast is disabled and DRM is enabled, you must provide an RF Domain ID.

9 From the **Minimum** drop-down list, select the minimum power level below which the power cannot be further reduced by the DRM.

10 From the **Maximum** drop-down list, select the maximum power level above which the power cannot be further increased by the DRM.

NOTE

Due to limited power control resolution, the actual power limits may differ slightly from the settings you define.

11 Click **Apply to selected APs**.

12 To save your changes, click **Save.**

13 To re-establish baseline settings, forcing the APs to go through the auto-channel selection process, click **Reset DRM**. This will cause all APs using DRM to reboot and rerun the auto-channel selection algorithm.

Modifying an Altitude AP's properties based on a default AP configuration

If you have an Altitude AP that is already configured with its own settings, but would like the Altitude AP to be reset to use the system's default AP settings, use the **Reset to Defaults** feature on the **AP Properties** tab.

To configure an Altitude AP with the system's default AP settings:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP** screen is displayed.

2 In the **Altitude AP** list, click the Altitude AP whose properties you want to modify. The **AP Properties** tab displays Altitude AP information.

3 Click **Reset to Defaults** to have the Altitude AP inherit the system's default AP settings. A pop-up window asking you to confirm the configuration change is displayed.

4 Click **OK** to confirm resetting the AP to the default settings.

Modifying the Altitude AP's default setting using the Copy to Defaults feature

You can modify the system's default AP settings by using the **Copy to Defaults** feature on the **AP Properties** tab. This feature allows the properties of an already configured AP to become the system's default AP settings.

To modify the system's default AP settings based on an already configured AP:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP** screen is displayed.

2 In the **Altitude AP** list, click the Altitude AP whose properties you want to become the system's default AP settings. The **AP Properties** tab displays Altitude AP information.

3 If applicable, modify the Altitude AP's properties. For more information, see "Modifying an Altitude AP's properties" on page 68.

4 Click **Copy to Defaults** to make this AP's configuration be the system's default AP settings. A pop-up window asking you to confirm the configuration change is displayed.

5 Click **OK** to confirm resetting the system's default AP settings.

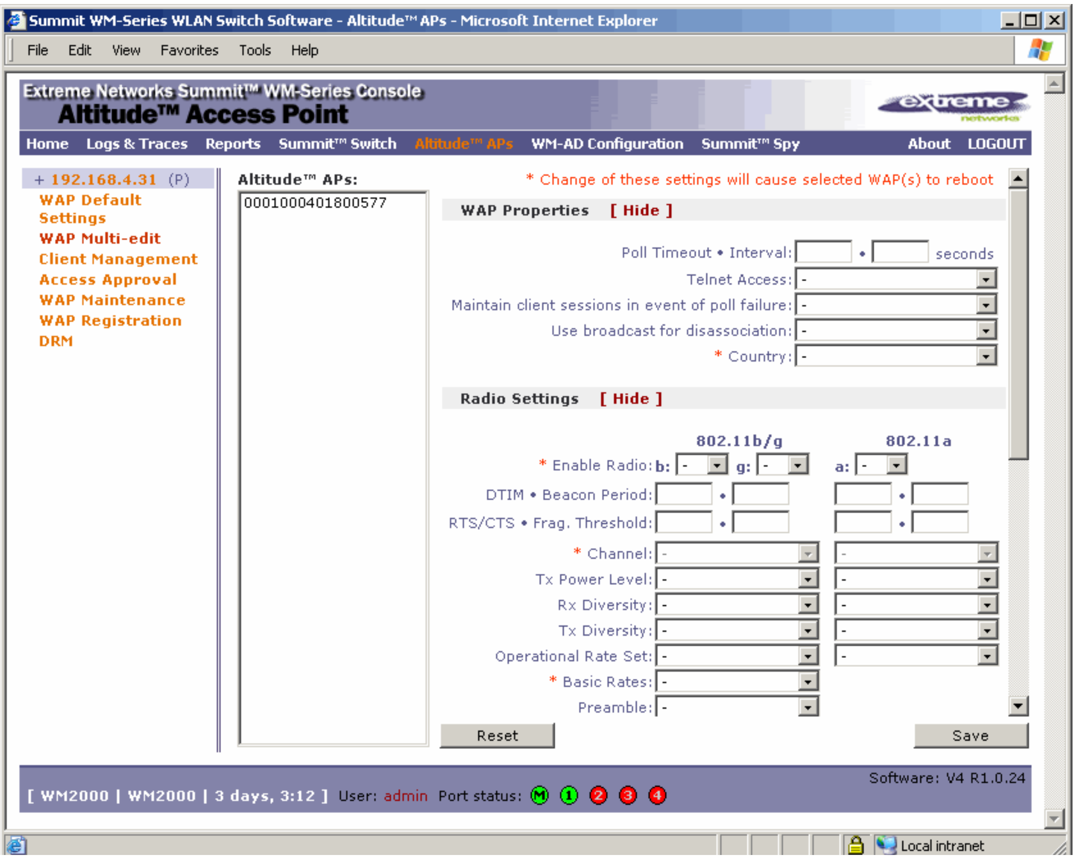
Configuring APs simultaneously

In addition to configuring APs individually, you can also configure multiple APs simultaneously by using the AP Multi-edit functionality.

To configure APs simultaneously:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP** screen is displayed.

2 In the left pane, click **WAP Multi-edit**.


Summit WM-Series WLAN Switch Software - Altitude™ APs - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Altitude™ Access Point
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
+ 192.168.4.31 (P)
WAP Default Settings
WAP Multi-edit
Client Management
Access Approval
WAP Maintenance
WAP Registration
DRM
Reset
Save
Local intranet

Altitude™ APs:
0001000401800577

* Change of these settings will cause selected WAP(s) to reboot

WAP Properties [Hide]

Poll Timeout • Interval: • seconds
Telnet Access: -
Maintain client sessions in event of poll failure: -
Use broadcast for disassociation: -
* Country: -

Radio Settings [Hide]

	802.11b/g	802.11a
* Enable Radio:	b: - g: -	a: -
DTIM • Beacon Period:	•	•
RTS/CTS • Frag. Threshold:	•	•
* Channel:	-	-
Tx Power Level:	-	-
Rx Diversity:	-	-
Tx Diversity:	-	-
Operational Rate Set:	-	-
* Basic Rates:	-	
Preamble:	-	

Software: V4 R1.0.24
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

3 In the **Altitude APs** list, select one or more APs to edit. To select multiple APs, select the appropriate APs from the list while pressing the CTRL key. The **Channel** drop-down list is not available if using the multi-edit feature.

NOTE

When using multi-edit configuration, any box or option that is not explicitly modified will not be changed by the update. The Altitude APs shown in the Altitude APs list can be from any version of the software. Attributes that are common between software versions are set on all Altitude APs. Attributes that are not common, are only sent to the AP versions to which the attributes apply. Attempting to set an attribute that does not apply for an AP will not abort the multi-edit operation.

4 Modify the configuration of the selected Altitude APs:

- **WAP Properties** – For more information, see "Modifying an Altitude AP's properties" on page 68.
- **Radio Settings** – For more information, see "Modifying the Altitude AP's radio properties" on page 70.
- **Static Configuration** – For more information, see "Setting up the Altitude AP using static configuration" on page 75.

5 In the **WAP Properties**, **Radio Settings**, and **Static Configuration** sections of the screen, select and enter the attributes you want to edit for all selected APs.

6 To save your changes, click **Save.**

Performing Altitude AP software maintenance

Periodically, the software used by the Altitude APs is altered for reasons of upgrade or security. The new version of the AP software is installed from the Summit WM series switch.

The software for each Altitude AP can be uploaded either immediately, or the next time the Altitude AP connects. Part of the Altitude AP boot sequence is to seek and install its software from the Summit WM series switch.

Although a number of the properties of each radio on an Altitude AP can be modified without requiring a reboot of the AP, a reboot is required after:

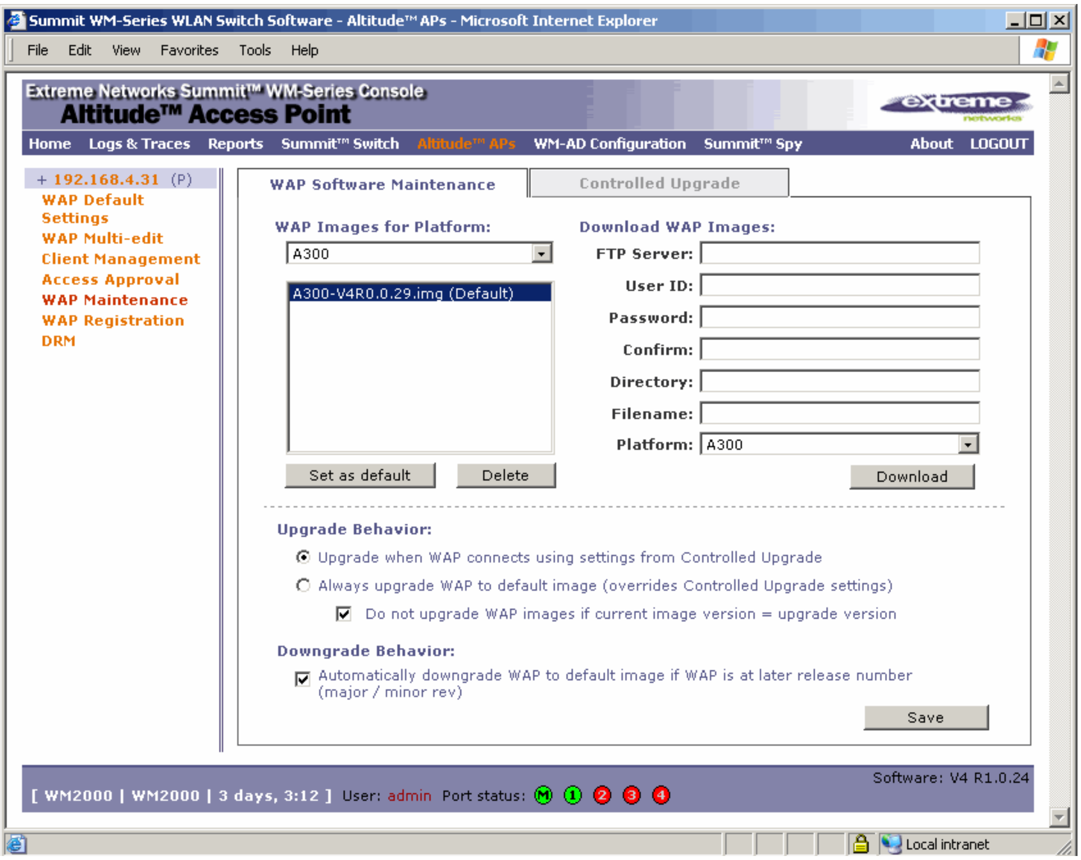
- Enabling or disabling either radio, or changing the radio channel between Auto and any fixed channel number
- Adding the Altitude AP to a WM-AD, or changing its radio assignment in a WM-AD

The Altitude AP keeps a backup copy of its software image. When a software upgrade is sent to the Altitude AP, the upgrade becomes the Altitude AP's current image and the previous image becomes the backup. In the event of failure of the current image, the Altitude AP will run the backup image.

To maintain the list of current Altitude AP software images:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** screen is displayed.

2 From the left pane, click **WAP Maintenance**. The **WAP Software Maintenance** tab is displayed.


Summit WM-Series WLAN Switch Software - Altitude™ APs - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Altitude™ Access Point
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
+ 192.168.4.31 (P)
WAP Default Settings
WAP Multi-edit
Client Management
Access Approval
WAP Maintenance
WAP Registration
DRM
WAP Software Maintenance
Controlled Upgrade
Set as default
Delete
Download
Save
Local intranet

WAP Images for Platform: A300

A300-V4R0.0.29.img (Default)

Download WAP Images:

FTP Server:

User ID:

Password:

Confirm:

Directory:

Filename:

Platform: A300

Upgrade Behavior:

● Upgrade when WAP connects using settings from Controlled Upgrade

○ Always upgrade WAP to default image (overrides Controlled Upgrade settings)

☑ Do not upgrade WAP images if current image version = upgrade version

Downgrade Behavior:

☑ Automatically downgrade WAP to default image if WAP is at later release number (major / minor rev)

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

3 From the **WAP Images for Platform** drop-down list select the appropriate platform.

4 To select an image to be the default image for a software upgrade, select it in the list, and then click **Set as default**.

5 In the **Upgrade Behavior** section, select one of the following:

- **Upgrade when WAP connects using settings from Controlled Upgrade** – The **Controlled Upgrade** tab is displayed. Controlled upgrade allows you to individually select and control the state of a WAP image upgrade: which APs to upgrade, when to upgrade, how to upgrade, and to which image the upgrade or downgrade should be done. Administrators decide on the levels of software releases that the equipment should be running.

- **Always upgrade WAP to default image (overrides Controlled Upgrade settings)** – Selected by default. Allows for the selection of a default revision level (firmware image) for all APs in the domain. As the WAP registers with the controller, the firmware version is verified. If it does not match the same value as defined for the default-image, the WAP is automatically requested to upgrade to the default-image.

6 Select the **Do not upgrade WAP images if current image version = upgrade version** checkbox to prevent an upgrade if current image version is the same as the upgrade version. Selecting this option overrides upgrade behavior.

7 Select the **Automatically downgrade the WAP to the default image if WAP is at later release number (major/minor rev)** checkbox to allow an older image to be installed if selected.

8 To save your changes, click **Save**.

To delete an Altitude AP software image:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** screen is displayed.

2 From the left pane, click **WAP Maintenance**. The **WAP Software Maintenance** tab is displayed.

3 From the **WAP Images for Platform** drop-down list, select the appropriate platform.

4 To select an image in the **WAP Images** list to delete, click it.

5 Click the **Delete** button. The image is removed from the list.

To download a new Altitude AP software image:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** screen is displayed.

2 From the left pane, click **WAP Maintenance**. The **WAP Software Maintenance** tab is displayed.

3 In the **Download WAP Images** list, type the following:

- **FTP Server –** The IP of the FTP server to retrieve the image file from.
- **User ID –** The user ID that the controller should use when it attempts to log in to the FTP server.
- **Password –** The corresponding password for the user ID.
- **Confirm –** The corresponding password for the user ID to confirm it was typed correctly.
- **Directory** – The directory on the server in which the image file that is to be retrieved is stored.
- **Filename –** The name of the image file to retrieve.
- **Platform –** The AP hardware type to which the image applies. The are several types of AP and they require different images.

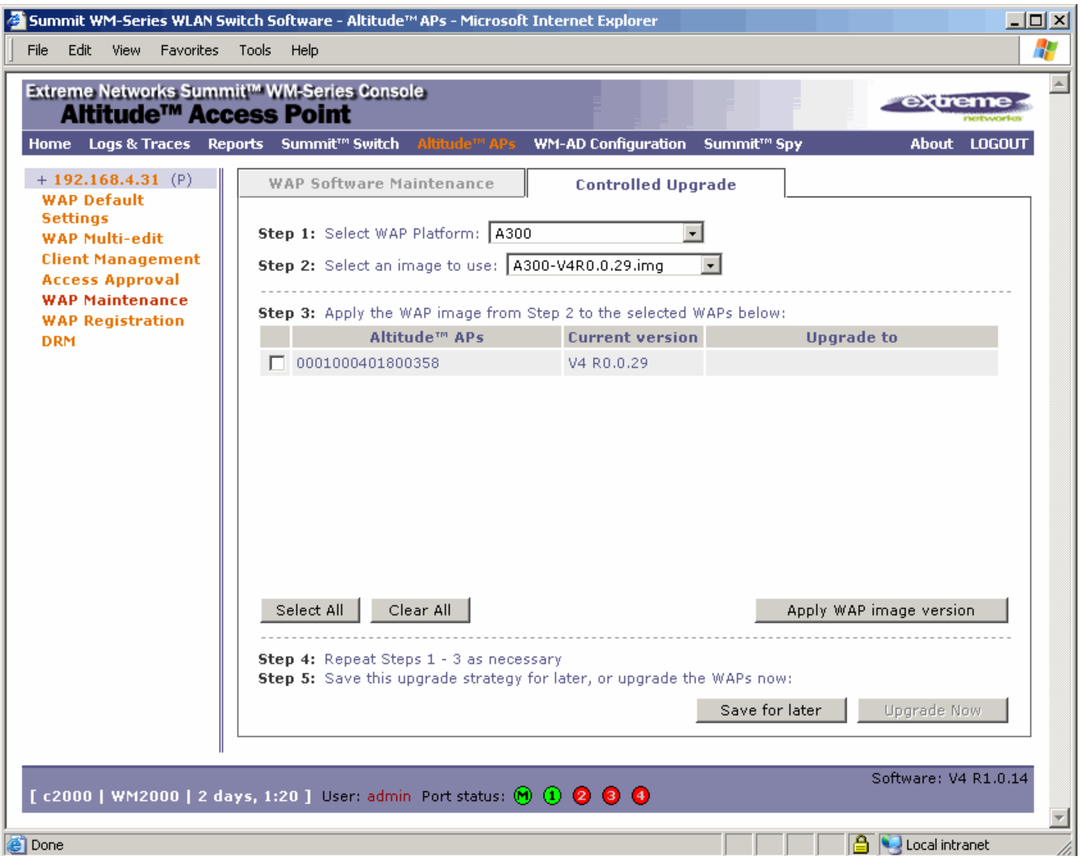
4 Click **Download**. The new software image is downloaded.

To define parameters for an Altitude AP controlled software upgrade:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** screen is displayed.

2 From the left pane, click **WAP Maintenance**. The **WAP Software Maintenance** tab is displayed.

3 Click the **Controlled Upgrade** tab.



Step 1: Select WAP Platform: A300

Step 2: Select an image to use: A300-V4R0.0.29.img

Step 3: Apply the WAP image from Step 2 to the selected WAPs below:

	Altitude™ APs	Current version	Upgrade to
□	0001000401800358	V4 R0.0.29	

Step 4: Repeat Steps 1 - 3 as necessary

Step 5: Save this upgrade strategy for later, or upgrade the WAPs now:

Software: V4 R1.0.14

[c2000 | WM2000 | 2 days, 1:20] User: admin Port status: M 1 2 3 4

NOTE

The Controlled Upgrade tab will appear only when the Upgrade Behavior is set to Upgrade when AP connects using settings from Controlled Upgrade on the AP Software Maintenance tab.

4 From the **Select WAP Platform** drop-down list, select the type of AP you want to upgrade.

5 From the **Select an image to use** drop-down list, select the software image you want to use for the upgrade.

6 In the list of registered **Altitude APs**, select the checkbox for each Altitude AP to be upgraded with the selected software image.

7 Click **Apply WAP image version**. The selected software image is displayed in the **Upgrade To** column of the list.

8 To save the software upgrade strategy to be run later, click **Save for later**.

9 To run the software upgrade immediately, click **Upgrade Now**. The selected Altitude AP reboots, and the new software version is loaded.

NOTE

The Always upgrade AP to default image checkbox on the WAP Software Maintenance tab overrides the Controlled Upgrade settings.

4 WM Access Domain Services (WM-AD)

This chapter describes WM Access Domain Services (WM-AD) concepts, including:

- WM-AD overview
- Setting up a WM-AD checklist
- Topology of a WM-AD
- RF assignment for a WM-AD
- Authentication for a WM-AD
- Filtering for a WM-AD
- Data protection on a WM-AD—WEP and WPA
- WM-AD global settings
- Setting up a new WM-AD

WM-AD overview

A WM-AD is an IP subnet designed to enable Altitude APs to interact with wireless devices. A WM-AD is similar to a regular IP subnet. A WM-AD has the following properties:

- Each WM-AD is assigned a unique identifier.
- Each WM-AD is assigned a Service Set Identifier (SSID). The SSID does not have to be unique.
- Each WM-AD is assigned a range of IP addresses for wireless devices. All of the wireless devices share the same IP address prefix—the part of the IP address that identifies the network and subnet.

  The IP addresses of the wireless devices are assigned dynamically by the Summit WM series switch's Dynamic Host Configuration Protocol (DHCP) server within the assigned range.

  NOTE

  If the WM-AD is in branch mode, the Summit WM series switch's DHCP server will not assign IP addresses to the wireless devices. For a routed WM-AD, you can allow the enterprise network's DHCP server to provide the IP addresses for the WM-AD by enabling DHCP Relay.

  The assigned addresses must be within range of the WM-AD definition and the controller must be defined in the network as the path for traffic delivery to the mobile units. For more information, see "Using a DHCP relay for the WM-AD" on page 104.

  These IP addresses are not virtual IP addresses. They are regular IP addresses and are unique over the network. These IP addresses are advertised to other hosts on the network to exchange traffic with the wireless devices in the WM-AD.
- A single overall filtering policy applies to all the wireless devices within the WM-AD. Additional filtering can be applied when the wireless user is authenticated by the Remote Authentication Dial-In User Service (RADIUS) server. This does not apply for a bridged WM-AD.
- When the Summit WM series switch creates a WM-AD, it also creates a virtual IP subnet for that WM-AD. This does not apply for a bridged WM-AD.

- Each WM-AD represents a mobility group that, when configured, can be carried across multiple Summit WM series switches. This does not apply for a bridged WM-AD.
- Each WM-AD also offers unique Authentication, Authorization and Accounting (AAA) services.

Setting up a WM-AD checklist

WM-AD provides a versatile means of mapping wireless networks to the topology of an existing wired network. When you set up a WM-AD on the Summit WM series switch, you are defining a subnet for a group of wireless device users. The WM-AD definition creates a virtual IP subnet where the Summit WM series switch acts as a default gateway to wireless devices.

In addition you can determine if the WM-AD is to apply for traffic bridging at the AP. This type of WM-AD requires specification of RF parameters and authentication parameters (if AAA type), although filtering specifications and topology specifications do not apply.

The Summit WM series switch WM200/2000 provides the option to define a WM-AD as locally bridged to a VLAN at the controller. To support that configuration, you must define which VLAN the WM-AD should bride to. With this configuration, it is possible that the controller is not involved in the IP address assignment for user addresses. Instead, the IP addresses for users are assigned directly by the DHCP infrastructure that services the VLAN.

NOTE

In a VLAN-bridged WM-AD, *the default configuration dictates that the controller is not the DHCP server for that segment. However, DHCP services can selectively be enabled, including DHCP Relay, allowing you to use the controller to become the default DHCP server for the VLAN, if applicable.*

Before defining a WM-AD, the following properties must be determined:

- A user access plan for both individual users and user groups
- The RADIUS attribute values that support the user access plan
- The location and identity of the Altitude APs that will be used on the WM-AD
- The routing mechanism to be used on the WM-AD
- For tunneled configurations mostly, the network addresses that the WM-AD will use
- A VLAN bridged WM-AD (at the controller) requires the specification of the IP address for the controller's own interface point (Port) on that VLAN. In addition, if the you elect to have the controller operate as the default DHCP server for the VLAN, the corresponding IP topology for that subnet must also be specified.
- The type of authentication for wireless device users on the WM-AD
- The specific filters to be applied to the defined users and user groups to control network access
- The quality of service (QoS) requirements
- What privacy mechanisms should be employed between the Altitude APs and the wireless devices
- Classification list for traffic priority. For example, whether the WM-AD is to be used for voice traffic and if voice traffic is to be given priority.
- Whether the WM-AD traffic is to be bridged directly to the network at the AP or tunneled to the controller for forwarding. Bridging at the AP is useful in branch office deployments in which APs must provide service even when the connection to the controller is unavailable.

User access plan

The user access plan should analyze the enterprise network and identify which users should have access to which areas of the network. What areas of the network should be separated? Which users can go out to the World Wide Web?

The Summit WM series switch, access points, and WLAN switch software system relies on authenticating users via a RADIUS server (or other authentication server). To make use of this feature, an authentication server on the network is required. Make sure that the server's database of registered users, with login identification and passwords, is current.

In the case of certificate-based installations, you must ensure that the proper user certificate profiles are setup on the RADIUS server.

NOTE

To deploy Summit WM series switch, access points, and WLAN switch software without a RADIUS server (and without authentication of users on the network), select SSID for network assignment (in the Topology screen). In the Authentication - Configure Captive Portal screen, select the No Captive Portal radio button. There will be no authentication of users, but Summit WM series switch, access points, and WLAN switch software is otherwise operational.

The user access plan should also identify the user groups in your enterprise, and the business structure of the enterprise network, such as:

- Department (such as Engineering, Sales, Finance)
- Role (such as student, teacher, library user)
- Status (such as guest, administration, technician)

For each user group, you should set up a filter ID attribute in the RADIUS server, and then associate each user in the RADIUS server to at least one filter ID name. You can define specific filtering rules, by filter ID attribute, that will be applied to user groups to control network access. Filtering is applied by the controller. Filter ID assignments is a configuration option, and not a requirement to setup per user filter ID definitions. If a filter is not returned by the Access-Accept confirmation for a particular user, the controller uses the default filter profile for the WM-AD as the applicable filter set.

Topology of a WM-AD

Before you decide if a WM-AD will participate in a VLAN and configure a WM-AD, define the global settings that will apply to all WM-AD definitions. For example, global settings can include identifying the location of the RADIUS servers and enabling priority traffic handling for voice-over-internet traffic and dynamic authorization server support.

The type of network assignment determines all the other factors of the WM-AD. There are two options for network assignment:

- **SSID**:
  - Has Captive Portal authentication, or no authentication
  - Requires restricted filtering rules before authentication

  - Requires filtering rules for group filter IDs after authentication. A default filter applies if a more specific filter is not indicated by the RADIUS Access-Accept response.
  - Used for a WM-AD supporting wireless voice traffic (QoS)
  - Used for a WM-AD supporting third-party APs
  - Has WEP and WPA-PSK privacy
- **AAA**:
  - Has 802.1x authentication
  - Requires filtering rules for group filter IDs and default filter. A definition of group filter IDs is optional. If a filter is not specified or not returned by the Access-Accept response, the default filter group is applied.
  - Has WEP and WPA privacy
  - Controller is involved in authenticating users. 802.1x packets for AAA assignment are forwarded by the AP to the controller, through to the RADIUS server.

Traffic behavior types

There are 3 traffic types available when setting up your WM-AD:

- Tunneled to SWM (routed)
- Bridged traffic locally at WAP
- Bridged traffic locally at SWM

You assign available Altitude APs, by radio, to the WM-AD. An Altitude AP radio is available for WM-AD assignment until it has been assigned to a maximum eight WM-ADs. The Summit WM series switch WM200/2000 can support up to 64 WM-ADs.

Each AP's radio can be assigned to any of the WM-ADs defined in the system, with up to 8 assignments per radio.

Once a WM-AD definition is saved, the Summit WM series switch updates this information on the Altitude AP. The WM-AD broadcasts the updates during beacon transmission, unless the SSID beacon is suppressed on the **Topology** tab.

The **Altitude AP Configuration** screen lists defined WM-ADs and which radio each has been assigned to.

On the **Topology** tab, define parameters for DHCP for IP address assignment. DHCP IP assignment is not applicable to Bridged at AP mode. DHCP assignment is disabled by default for Bridged to VLAN mode. However, you can enable DHCP server/relay functionality to have the controller service the IP addresses for the VLAN (and wireless users).

You can also configure this WM-AD for management traffic or for third-party APs.

RF assignment for a WM-AD

The second step in setting up a WM-AD is to configure the RF assignment for the WM-AD. From the **RF** tab you assign APs to a WM-AD and SSID definitions.

Authentication for a WM-AD

The third step in setting up a WM-AD is to configure the authentication mechanism for the WM-AD. The authentication mechanism depends on the network assignment. In addition, all WM-AD definitions can include authentication by Media Access Control (MAC) address. Authentication by MAC address provides a method of access control for a user as it associates with the AP based on the device's MAC address.

Authentication with SSID network assignment

If network assignment is SSID, there are two authentication options:

- **None** – This authentication method is the default for a new SSID assignment WM-AD. Authentication WM-AD, unless MAC-based authorization is used, the default filter is applied, not the non-authentication filter. For more information, see "Filtering for a WM-AD" on page 90.
- **Captive Portal** – This authentication method employs a Web redirection which directs a user's Web session to an authentication server. Typically, the user must provide their credentials (userID, password) to be authenticated. The Captive Portal redirection operation will redirect any Web page requests corresponding to targets not explicitly allowed by the non-authenticated filter. The redirection will instruct the user's Web page to contact the defined authentication Web server. You must ensure that the authentication Web server is explicitly listed as an allow destination in order for traffic to access it.

  The Summit WM series switch supports two modes of Captive Portal authentication:

  - **Internal Captive Portal** – The controller's own Captive Portal authentication page (configured as an editable form) is used to request user credentials.
  - **External Captive Portal** – An entity outside of the Summit WM series switch is responsible for handling the user authentication process, presenting the credentials request forms and performing user authentication procedures. The controller is then informed of the authentication results via its Business Echosystem's interfaces.

  Four authentication types are supported for Captive Portal authentication:

  - Password Authentication Protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)
  - Windows-specific version of CHAP (MS CHAP)
  - MS CHAP v2 (Windows-specific version of CHAP, version 2)

  For Captive Portal authentication, the RADIUS server must support the selected authentication type: PAP, CHAP (RFC2484), MS-CHAP (RFC2433), or MS-CHAPv2 (RFC2759).

Authentication with AAA (802.1x) network assignment

If network assignment is AAA with 802.1x authentication, the wireless device user requesting network access must first be authenticated. The wireless device's client utility must support 802.1x. The user's request for network access along with login identification or a user profile is forwarded by the Summit WM series switch to a RADIUS server. Summit WM series switch, access points, and WLAN switch software supports the following authentication types:

- **Extensible Authentication Protocol - Transport Layer Security (EAP-TLS)** – Relies on client-side and server-side certificates to perform authentication. Can be used to dynamically generate a Pairwise Master Key for encryption.

- **Extensible Authentication Protocol with Tunneled Transport Layer Security (EAP-TTLS) –** Relies on mutual authentication of client and server through an encrypted tunnel. Unlike EAP-TLS, it requires only server-side certificates. The client uses PAP, CHAP, or MS-CHAPv2 for authentication.
- **Protected Extensible Authentication Protocol (PEAP) –** Is an authentication protocol similar to TTLS in its use of server side certificates for server authentication and privacy and its support for a variety of user authentication mechanisms.

For 802.1x, the RADIUS server must support RADIUS extensions (RFC2869).

Until the access-accept is received from the RADIUS server for a specific user, the user is kept in an unauthenticated state. 802.1x rules dictate no other packets other than EAP are allowed to traverse between the AP and the Summit WM series switch until authentication completes. Once authentication is completed (access-accept is received), the user's client is then allowed to proceed with IP services, which typically implies the request of an IP address via DHCP. In addition, the definition of a specific filter ID is optional configuration. If a specific filter ID is not defined or returned by the access-accept operation, the Summit WM series switch assigns the WM-AD' default filter for authenticated users.

NOTE

The Summit WM series switch only assigns the device's IP after the client requests one.

Both Captive Portal and AAA (802.1x) authentication mechanisms in Summit WM series switch, access points, and WLAN switch software rely on a RADIUS server on the enterprise network. You can identify and prioritize up to three RADIUS servers on the Summit WM series switch—in the event of a failover of the active RADIUS server, the Summit WM series switch will poll the other servers in the list for a response. Once an alternate RADIUS server is found, it becomes the active RADIUS server, until it either also fails, or the administrator redefines another.

Filtering for a WM-AD

The WM-AD capability provides a technique to apply policy, to allow different network access to different groups of users. This is accomplished by packet filtering.

After setting authentication, define the filtering rules for the filters that apply to your network and the WM-AD you are setting up. Several filter types are applied by the Summit WM series switch:

- **Exception filter –** Protect access to a system's own interfaces, including the WM-AD's own interface. WM-AD exception filters are applied to user traffic intended for the Summit WM series switch's own interface point on the WM-AD. These filters are applied after the user's specific WM-AD state assigned filters.
- **Non-authenticated filter with filtering rules that apply before authentication –** Controls network access and to direct users to a Captive Portal Web page for login.
- **Group filters, by filter ID, for designated user groups –** Controls access to certain areas of the network, with values that match the values defined for the RADIUS filter ID attribute.
- **Default filter –** Controls access if there is no matching filter ID for a user.

Within each type of filter, define a sequence of filtering rules. The filtering rule sequence must be arranged in the order that you want them to take effect. Each rule is defined to allow or deny traffic in either direction:

- **In –** From a wireless device in to the network
- **Out –** From the network out to a wireless device

Final filter rule

The final rule in any filter should act as a catch-all for any traffic that did not match a filter. This final rule should either allow all or deny all traffic, depending on the requirements for network access. For example, the final rule in a non-authenticated filter for Captive Portal is typically deny all. A final allow all rule in a default filter will ensure that a packet is not dropped entirely if no other match can be found.

A default rule of deny all is automatically created by the system for initial filter definitions. The administrator can change the action to allow all. However, a default filter rule cannot be removed. Since a default filter rule provides a catch-all default behavior for packet handling, all applicable user defined filter rules must be defined prior to this rule.

Each rule can be based on any one of the following:

- Destination IP address or any IP address within a specified range that is on the network subnet (as a wildcard)
- Destination ports, by number and range
- Protocols (UDP, TCP, etc.)

Filtering sequence

The filtering sequence depends on the type of authentication used:

- No authentication (network assignment by SSID)

  Only the default filter will apply. Specific network access can be defined.
- Authentication by captive portal (network assignment by SSID)

  The non-authenticated filter will apply before authentication. Specific network access can be defined. The filter should also include a rule to allow all users to get as far as the Captive Portal Web page where the user can enter login identification for authentication. When authentication is returned, the filter ID group filters are applied. If no filter ID matches are found, then the default filter is applied. The filter ID group is an optional behavior specification. If a filter ID is not returned, or an invalid one is returned, the default filter group is applied.
- Authentication by AAA (802.1x)

  AAA assignment requires that user authentication is completed using the 802.1x/EAP protocol before a user is granted access to a network resource. Therefor, the enforcement of non-authenticated traffic rules is not applicable. When authentication is returned, then the filter ID group filters are applied. A WM-AD can have a subgoup with Login-LAT-Group ID that has its own filtering rules. The Login-LAT-Group indicates that a user session should be associated with a more specific WM-AD (a child WM-AD). The sub-WM-AD provides a different topology definition than the parent WM-AD, as well as having its own set of filter definitions. Filter IDs returned in association with a Login-LAT-Group definition are applied to the user, in relation to the sub-WM-AD indicated by the Login-LAT-Group specification. If no filter ID matches are found, then the default filter is applied.

The following is a high-level description of how Summit WM series switch filters traffic:

Step One – The Summit WM series switch attempts to match each packet of a WM-AD to the filtering rules that apply to the wireless device user.

Step Two – If a filtering rule is matched, the operation to allow or deny is executed.

Step Three – The next packet is fetched for filtering.

Data protection on a WM-AD—WEP and WPA

On wireless and wired networks, data is protected by encryption techniques. The type of data protection that is available depends on the WM-AD assignment mode:

- **SSID** – Only WEP and WPA (1or 2)-PSK privacy types are available
- **AAA** – WEP, Dynamic WEP, and WPA (1 or 2) privacy types are available

Data protection encryption techniques

- **Wired Equivalent Privacy (WEP)** – WEP encrypts data sent between wireless nodes. Each node must use the same encryption key.
- **Wi-Fi Protected Access Privacy (WPA v.1 and v.2)** – Encryption is by Advanced Encryption Standard (AES) or by Temporal Key Integrity Protocol (TKIP). Two modes are available:
  - **Enterprise** – Specifies 802.1x authentication and requires an authentication server
  - **Pre-Shared Key (PSK)** – Relies on a shared secret. The PSK is a shared secret (pass-phrase) that must be entered in both the Altitude AP or router and the WPA clients.

WM-AD global settings

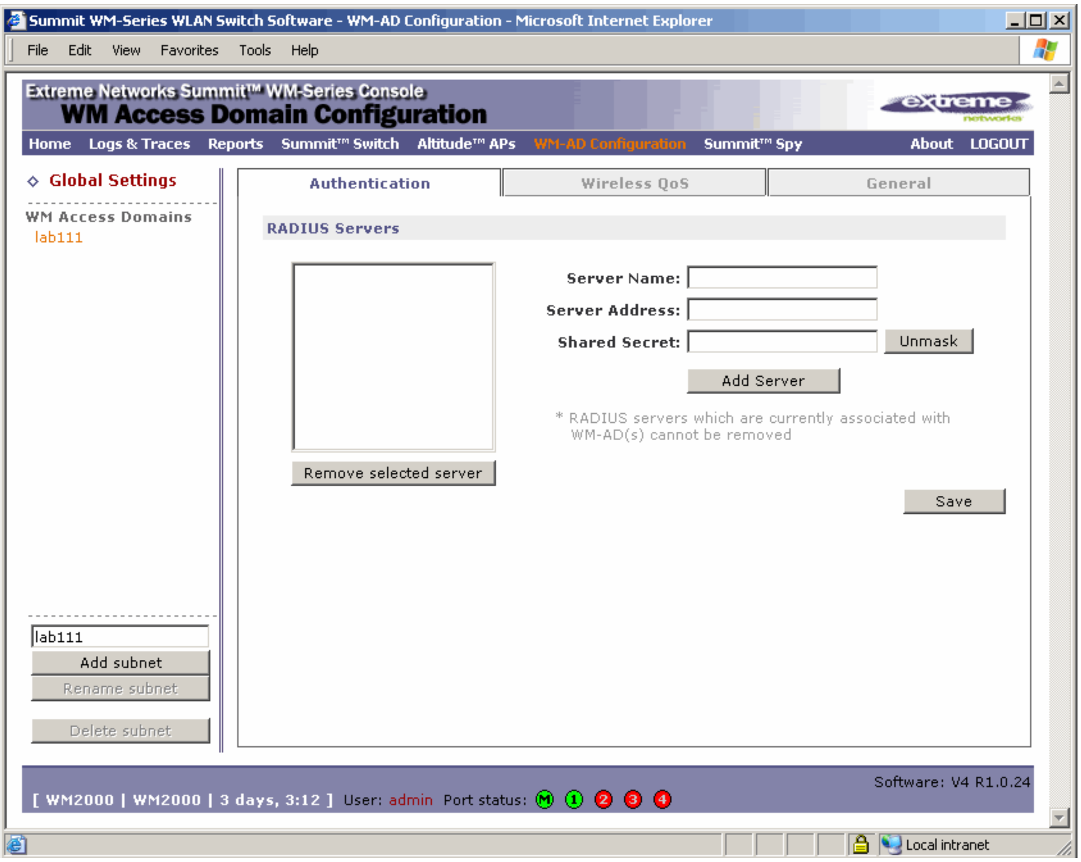
Before defining a specific WM-AD, define the global settings that will apply to all WM-AD definitions. These global settings include:

- Identify the location and password of RADIUS servers on the enterprise network. The defined servers appear as available choices when you set up the authentication mechanism for each WM-AD.
- Define the shared secret used to encrypt the Pairwise Master Key (PMK) for WPA2 v.2 pre-authentication between Summit WM series switches on the network.
- Adjust admission control thresholds. Admission control thresholds protect admitted traffic against overloads, provides distinct thresholds for VO and VI, and distinct thresholds for roaming and new streams.

To define RADIUS servers for WM-AD global settings:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domains** list is displayed.

2 In the left pane, click **Global Settings**. The **Authentication** tab is displayed.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domains
lab111
Authentication
Wireless QoS
General
RADIUS Servers
Server Name:
Server Address:
Shared Secret:
Unmask
Add Server
Remove selected server
Save
lab111
Add subnet
Rename subnet
Delete subnet
Local intranet

* RADIUS servers which are currently associated with WM-AD(s) cannot be removed

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

3 To define a RADIUS server available on the network, do the following:

- In the **Server Name** box, type a name.
- In the **Server Address** box, type the IP address.
- In the **Shared Secret** box, type the password that is required in both directions. This password is used to validate the connection between controller and the RADIUS server.

4 In order to proofread your password before saving the configuration, click **Unmask**. The password is displayed. To mask the password, click **Mask**.

This precautionary step is highly recommended in order to avoid an error, later, when the Summit WM series switch attempts to communicate with the RADIUS server.

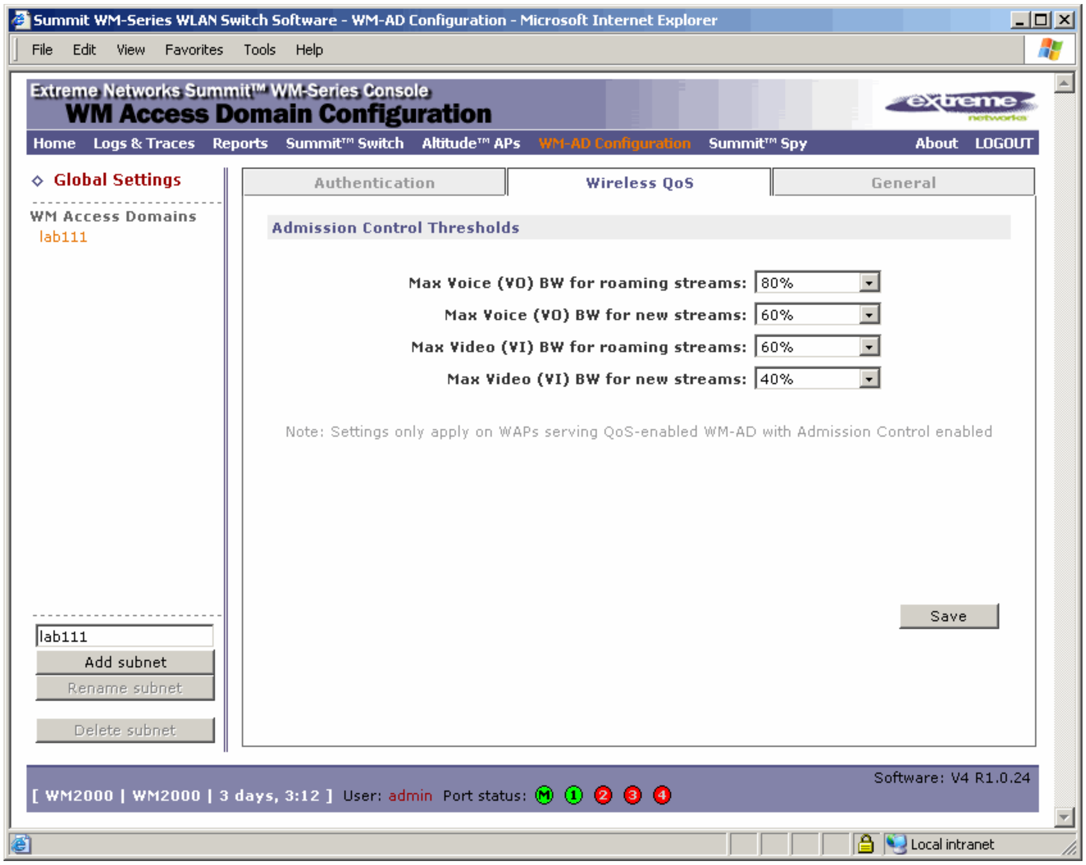
5 To add the server to the list, click **Add**.

6 To remove a server, select the server in the list and click **Remove selected server**.

7 To save your changes, click **Save**.

To define admission control thresholds for WM-AD global settings:

1. From the main menu, click **WM Access Domain Configuration**. The **WM Access Domains** list is displayed.
2. In the left pane, click **Global Settings**. The **Authentication** tab is displayed.
3. Click the **Wireless QoS** tab.



Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domains
lab111
Authentication
Wireless QoS
General
Add subnet
Rename subnet
Delete subnet
Save
Local intranet

Admission Control Thresholds

Max Voice (VO) BW for roaming streams: 80%

Max Voice (VO) BW for new streams: 60%

Max Video (VI) BW for roaming streams: 60%

Max Video (VI) BW for new streams: 40%

Note: Settings only apply on WAPs serving QoS-enabled WM-AD with Admission Control enabled

lab111

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

4. Using the percentage drop-down lists, define the thresholds for the following:
   - **Max Voice (VO) BW for roaming streams –** The maximum allowed overall bandwidth on the new AP when a client with an active voice stream roams to a new AP and requests admission for the voice stream.
   - **Max Voice (VO) BW for new streams –** The maximum allowed overall bandwidth on an AP when an already associated client requests admission for a new voice stream.
   - **Max Video (VI) BW for roaming streams –** The maximum allowed overall bandwidth on the new AP when a client with an active video stream roams to a new AP and requests admission for the video stream.
   - **Max Video (VI) BW for new streams –** The maximum allowed overall bandwidth on an AP when an already associated client requests admission for a new video stream.

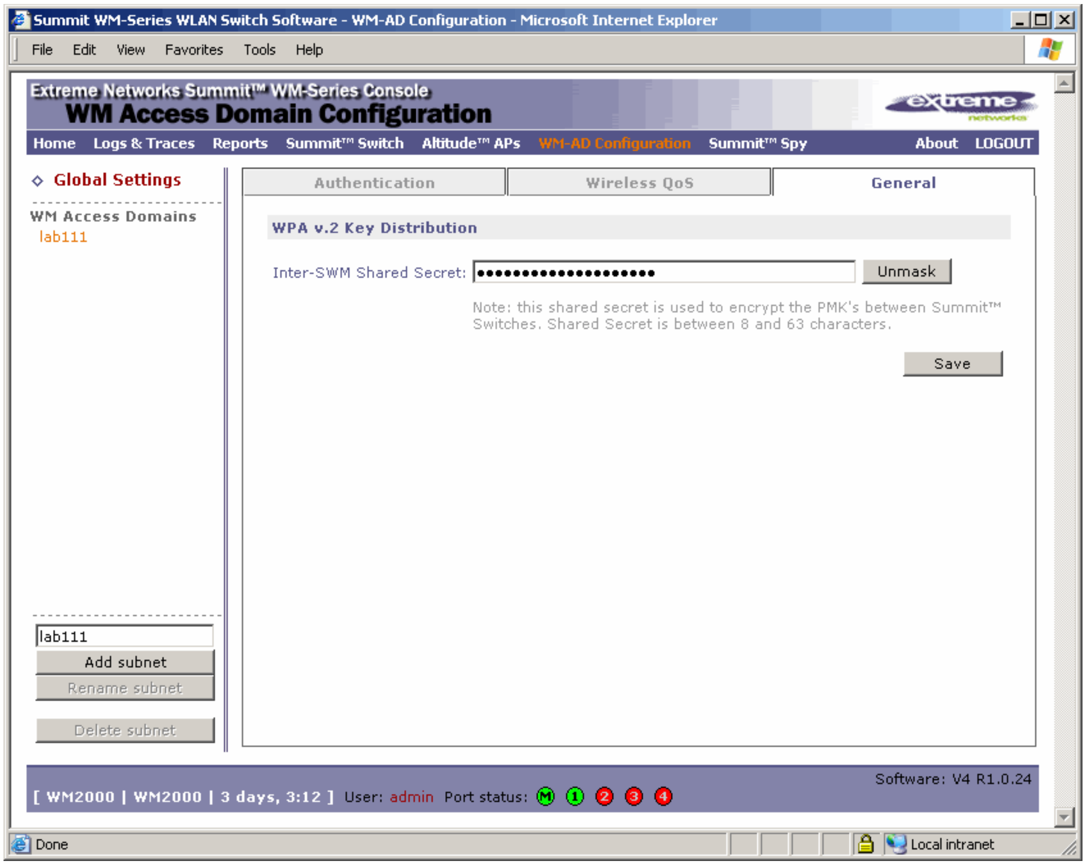
   These global QoS settings apply to all APs that serve QoS enabled WM-ADs with admission control.
5. To save your changes, click **Save**.

To define inter-Summit WM series switch shared secret for WM-AD global settings:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domains** list is displayed.

2 In the left pane, click **Global Settings**.

3 Click the **General** tab.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domains
lab111
Authentication Wireless QoS General
WPA v.2 Key Distribution
Inter-SWM Shared Secret:
Unmask
Save
Add subnet
Rename subnet
Delete subnet
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4
Software: V4 R1.0.24
Done
Local intranet

Inter-SWM Shared Secret: ••••••••••••••••••••

Note: this shared secret is used to encrypt the PMK's between Summit™ Switches. Shared Secret is between 8 and 63 characters.

lab111

4 In the **Inter-SWM Shared Secret** box, type a password between 8 and 63 characters long, to be used between Summit WM series switches. The shared secret is to encrypt pre-shared keys that have to be moved between controllers for mobility. The same shared secret must also be defined on the other Summit WM series switches on the network.

5 In order to proofread your password before saving the configuration, click **Unmask**. The password is displayed. To mask the password, click **Mask**.

This precautionary step is highly recommended in order to avoid an error, later, when the Summit WM series switch attempts to communicate with the RADIUS server.

6 To save your changes, click **Save**.

Setting up a new WM-AD

Now that you are familiar with the WM-AD concepts, you can now set up a new WM-AD. Setting up a new WM-AD involves the following general steps:

- Step one – Create a WM-AD name
- Step two – Define the topology parameters
- Step three – Configure the WM-AD

For information on setting up a new WM-AD, see Chapter 5, "WM Access Domain Services configuration."

5 WM Access Domain Services configuration

This chapter discusses WM Access Domain Services (WM-AD) configuration, including:

- Topology for a WM-AD
- Assigning Altitude AP radios to a WM-AD
- Authentication for a WM-AD
- Defining accounting methods for a WM-AD
- Defining RADIUS filter policy for WM-ADs and WM-AD groups
- Configuring filtering rules for a WM-AD
- Enabling multicast for a WM-AD
- Configuring privacy for a WM-AD
- Defining a WM-AD with no authentication
- Defining priority level and service class for WM-AD traffic
- Working with Quality of Service (QoS)
- Configuring the QoS policy on a WM-AD
- Bridging traffic locally

Setting up a WM-AD defines a virtual IP subnet for a group of wireless device users, where the Summit WM series switch acts as a default gateway to wireless devices. For each WM-AD, you define its topology, authentication, accounting, RADIUS servers, filtering, multicast parameters, privacy and policy mechanism. When you set up a new WM-AD, additional tabs appear only after you save the topology.

A critical topology option to define for a WM-AD is the WM-AD type:

- **Routed WM-AD** – User traffic is tunneled to the Summit WM series switch. (This is the default setup.)
- **Bridged at the AP WM-AD** – User traffic is directly bridged to a VLAN at the AP network point of access (switch port).
- VLAN bridged WM-AD – User traffic is tunneled to the Summit WM series switch and is directly bridged at the controller to a specific VLAN. WIth this WM-AD type, mobile users become a natural extension of a VLAN subnet.

Setting up a new WM-AD involves the following general steps:

- Step one – Create a WM-AD name
- Step two – Define the topology parameters
- Step three – Configure the WM-AD

Before you can define the WM-AD topology parameters and configure the WM-AD, you must first create a new WM-AD name.

To create a new WM-AD name:

1. From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.
2. In the left pane, type a name that will identify the new WM-AD in the **Add subnet** box, and then click **Add subnet**. The name is displayed in the **WM-AD** list. The **Topology** screen is displayed.

The following sections describe in detail how to define the WM-AD topology parameters and configure the WM-AD.

Topology for a WM-AD

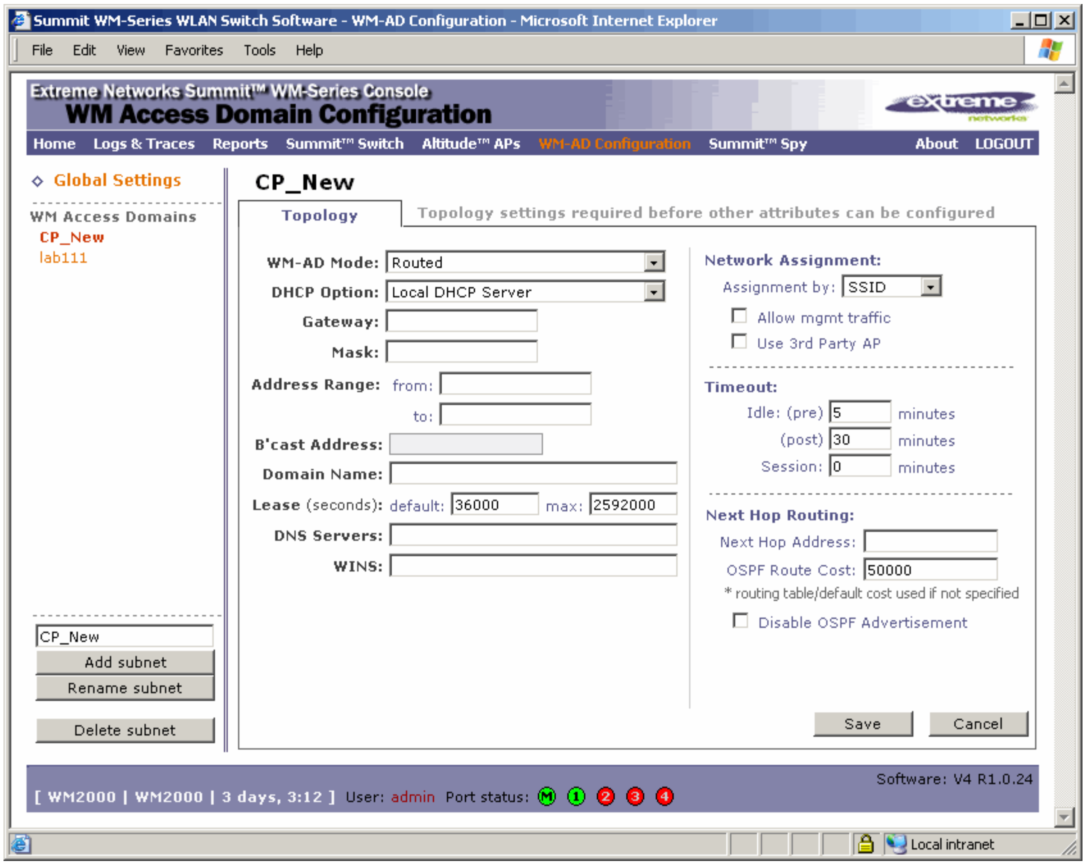
In the Topology screen, the key choice for a WM-AD is the type of network assignment, which determines all the other factors of the WM-AD. When you have completed defining the topology for your WM-AD, save the topology settings. Once your topology is saved, you can then access the remaining WM-AD tabs and continue configuring your WM-AD.

There are two options for network assignment:

- **SSID –** The SSID determines the WM-AD to which a user profile will be assigned (user topology/IP, filters):
  - Has Captive Portal authentication, or no authentication (as well as MAC-based authentication).
  - Requires restricted filtering rules before authentication and, after authentication, filtering rules for group filter IDs.
  - Is used for a WM-AD supporting wireless voice traffic (QoS).
  - Is used for a WM-AD supporting third-party APs.
  - Has WEP and WPA-PSK privacy.
- **AAA** (Authentication, Authorization and Accounting):
  - has 802.1x authentication (as well as MAC-based authentication).
  - requires filtering rules for group filter IDs and default filter.
  - has Dynamic WEP and WPA (WPA v.1 and WPA v.2) privacy.

Configuring topology for a WM-AD for Captive Portal

The section describes how to set up a WM-AD for Captive Portal. The **RF** tab, where you assign APs to WM-ADs, is not accessible until the topology for the WM-AD has been configured and saved.



CP_New

Topology settings required before other attributes can be configured

WM-AD Mode: Routed

DHCP Option: Local DHCP Server

Gateway:

Mask:

Address Range: from: to:

B'cast Address:

Domain Name:

Lease (seconds): default: 36000 max: 2592000

DNS Servers:

WINS:

Network Assignment:

Assignment by: SSID

□ Allow mgmt traffic

□ Use 3rd Party AP

Timeout:

Idle: (pre) 5 minutes

(post) 30 minutes

Session: 0 minutes

Next Hop Routing:

Next Hop Address:

OSPF Route Cost: 50000

* routing table/default cost used if not specified

□ Disable OSPF Advertisement

CP_New

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

To create an SSID for Captive Portal WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to create an SSID for. The **Topology** tab is displayed.

3 From the **Assignment by** drop-down list, select **SSID**.

Defining session timeout parameters

The Summit WM series switch allows a client to associate to the AP and exist on the network without having authentication. Every associated user has a user session tracked by the Summit WM series switch from the time of association with the AP. Users can be temporarily (or longer for SSID assigned WM-ADs) be in the non-authenticated state. Pre timeout is the maximum amount of time allowed to elapse from the last time any traffic was received by the system for an un-authenticated user. For example, a user may have disconnected from the system (shutdown the device, moved out of range, etc.). A pre timeout expires and cleans up the session.

The post timeout is the max amount of time that is allowed to elapse from the last time any traffic was received for an authenticated user. For example, a user may have disconnected from the system and is no longer be connected. A post timeout expires and cleans up the session.

A client that exceeds either the pre or post timeout value will be forced to disassociate.

The session timer defines the maximum amount of time a session is allowed to be connected to the system. The session timer is particularly useful in pay-per-use models. When the lifetime of the session reaches the defined limit, the session is expired and cleaned up. A user would have to re-authenticate with the system to continue to receive network services.

NOTE

The WM-AD timeout parameters define the default timers applicable to session management within the WM-AD. However, RADIUS authentication (access-accept) may return specific timers applicable to the particular user. A RADIUS returned value overwrites the WM-AD default values for the specific user.

In addition, a zero (0) value for any of the timers indicates a non-applicable value. Therefor, the corresponding timer is not enforced.

To define the session timeout parameters for a WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to define the session timeout parameters for. The **Topology** tab is displayed.

3 In the **Idle (pre)** box, type the number of minutes that a client is allowed to be idle on the WM-AD before authentication.

4 In the **Idle (post)** box, type the number of minutes that a client is allowed to be idle on the WM-AD after authentication.

5 In the **Session** box, type the maximum time limit of a session. If you do not provide a Session value, there is no time limit.

Enabling management traffic

If management traffic is enabled for a WM-AD, it overrides the built-in exception filters that prohibit traffic on the Summit WM series switch data interfaces. For more information, see "Configuring filtering rules for a WM-AD" on page 123.

To enable management traffic on a WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to enable management traffic for. The **Topology** tab is displayed.

3 Select the **Allow mgmt traffic** checkbox.

Enabling third-party APs on a WM-AD

Configuring a WM-AD for third-party APs is only available with SSID network assignment. Use this function as part of the process defined in Chapter 7, "Working with third-party APs."

A third-party AP WM-AD allows for the specification of a segregated subnet by which non-Extreme Altitude APs are used to provide RF services to users while still utilizing the Summit WM series switch for user authentication and user policy enforcement.

NOTE

Third-party AP devices are not fully integrated with the system and therefore must be managed individually to provide the correct user access characteristics. Also, third-party AP devices must be defined in bridge mode so that user traffic is directly transposed to the third-party AP subnet and picked up by the Summit WM series switch for forwarding and policy enforcement.

To enable third-party APs on a WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to enable third-party APs for. The **Topology** tab is displayed.

3 Select the **Use 3rd Party AP** checkbox.

The definition of third-party AP identification parameters allows the system to be able to differentiate the third-party AP device (and corresponding traffic) from user devices on that segment. Devices identified as third-party APs are considered pre-authenticated, and are not required to complete the corresponding authentication verification stages defined for users in that segment (typically Captive Portal enforcement).

In addition, third-party APs have a specific set of filters (third-party) applied to them by default, which allows the administrator to provide different traffic access restrictions to the third-party AP devices for the users that use those resources. The third-party filters could be used to allow access to third-party APs management operations (for example, HTTP, SNMP).

4 To save your changes, click **Save**.

Defining a next hop route and OSPF advertisement for a WM-AD

The next hop definition allows the administrator to define a specific host as the target for all non-WM-AD targeted traffic for users in a WM-AD. The next hop IP identifies the target device to which all WM-AD (user traffic) will be forwarded to. Next-hop definition supersedes any other possible definition in the routing table.

If the traffic destination from a wireless device on a WM-AD is outside of the WM-AD, it is forwarded to the next hop IP address, where this router applies policy and forwards the traffic. This feature applies to unicast traffic only. In addition, you can also modify the Open Shortest Path First (OSPF) route cost.

OSPF is an interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm. Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately distributes the information to all other hosts in the network so that all will have the same routing table information. The host using OSPF sends only the part that has changed, and only when a change has taken place.

To define a next hop route and OSPF advertisement:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to define a next-hop route for. The **Topology** tab is displayed.

3 In the **Next Hop Address** box, type the IP address of the next hop router on the network through which you wish all traffic on this WM-AD to be directed.

4 In the **OSPF Route Cost** box, type the OSPF cost of reaching the WM-AD subnet.

The OSPF cost value provides a relative cost indication to allow upstream routers to calculate whether or not to use the controller as a better fit or lowest cost path to reach devices in a particular network. The higher the cost, the less likely of the possibility that the controller will be chosen as a route for traffic, unless that controller is the only possible route for that traffic.

5 To disable OSPF advertisement on this WM-AD, select the **disable OSPF Advertisement** checkbox.

Defining the IP address for the WM-AD (for the DHCP server on the controller)

Bridged at the AP WM-ADs do not require the definition of a corresponding IP address definition for the WM-AD since all traffic for users in that WM-AD will be directly bridged by the AP at the local network point of attachment (VLAN at AP port).

The IP address definition is only required for a routed WM-AD or VLAN bridged WM-AD.

To define the IP address for the WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to define the IP address for. The **Topology** tab is displayed.

3 In the **Gateway** box, type the Summit WM series switch's own IP address in that WM-AD.

This IP address is the default gateway for the WM-AD. The Summit WM series switch advertises this address to the wireless devices when they sign on. For routed WM-ADs, it corresponds to the IP address that is communicated to MUs (in the WM-AD) as the default gateway for the WM-AD subnet. (MUs target the Summit WM series switch's interface in their effort to route packets to an external host).

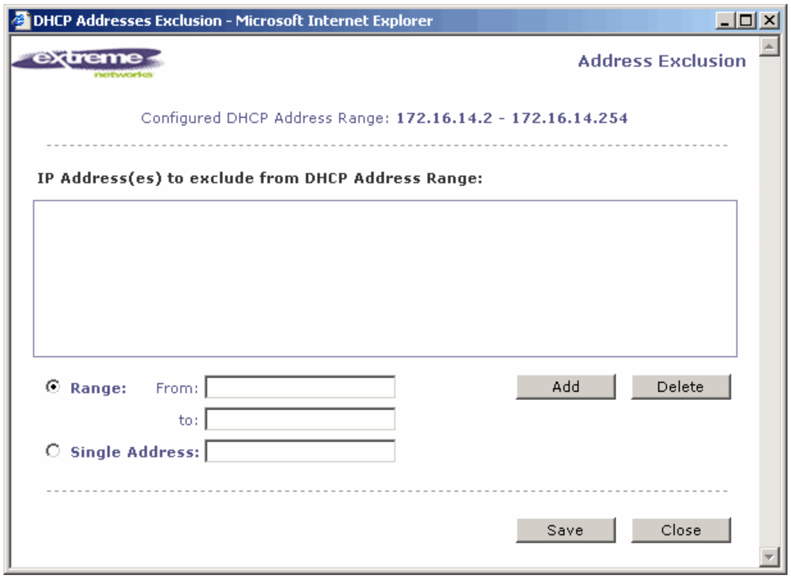
For a VLAN bridged WM-AD, the IP address corresponds to the Summit WM series switch's own point of presence on the VLAN. In this case, the controller's interface is typically not the gateway for the subnet. The gateway for the subnet is the infrastructure router defined to handle the VLAN.

4 In the **Mask** box, type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).

The following values to DHCP configuration are only applicable for configurations if the controller is the DHCP server for users in the WM-AD—a routed WM-AD or a VLAN bridged WM-AD with DHCP enabled (by default, DHCP is disabled). These values are not visible for a bridged at AP WM-AD or a VLAN bridged WM-AD with DHCP disabled (by default, DHCP is disabled).

The **Address Range** boxes (from and to) populate automatically with the range of IP addresses to be assigned to wireless devices using this WM-AD, based on the IP address you provided.

- To modify the address in the **Address Range from** box, type the first available address.
- To modify the address in the **Address Range to** box, type the last available address.
- If there are specific IP addresses to be excluded from this range, click **Exclusion(s)**. The DHCP Address Exclusion subscreen is displayed.



Configured DHCP Address Range: 172.16.14.2 - 172.16.14.254

IP Address(es) to exclude from DHCP Address Range:

- In the DHCP Address Exclusion subscreen, do one of the following:
  - To specify an IP range, type the first available address in the **From** box and type the last available address in the **to** box. Click **Add** for each IP range you provide.
  - To specify a IP address, select the **Single Address** option and type the IP address in the box. Click **Add** for each IP address you provide.
- To save your changes, click **Save**. The DHCP Address Exclusion subscreen closes.

5 The **Broadcast Address** box populates automatically based on the Gateway IP address and subnet mask of the WM-AD.

6 In the **Domain Name** box, type the external enterprise domain name.

Modifying time limits for IP assignments

The following procedure is only applicable for configurations if the controller is the DHCP server for users in the WM-AD—a routed WM-AD or a VLAN bridged WM-AD with DHCP enabled (by default, DHCP is local). These values are not visible for a bridged at AP WM-AD or a VLAN bridged WM-AD with DHCP disabled (by default, DHCP is disabled).

Time limits for IP assignments dictate the default and the maximum time limits a wireless device can keep the DHCP server-assigned IP address.

To modify time limits for IP assignments:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to set time limits for. The **Topology** tab is displayed.

3 In the **Lease default** box, type the default time limit. The default time limit dictates how long a wireless device can keep the DHCP server assigned IP address. The default value is 36000 seconds (10 hours).

4 In the **Lease max** box, type the maximum time limit. The default time limit is 2539000 seconds (approximately 705 hours or 29 days).

Setting the name server configuration

Although this procedure could also apply to any WM-AD type, normally these settings are defined in the context of DHCP definitions and therefor these values are not available for configurations if DHCP service is not defined.

A VLAN bridged WM-AD has an option to define the DHCP behavior for the WM-AD. By default, the DHCP service is disable although the administrator can elect to have the controller's WM-AD interface on the VLAN become either the actual DHCP server (enable DHCP) or become the relay agent for DHCP requests.

To set the name server configuration:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to set the name server configuration for. The **Topology** tab is displayed.

3 In the **DNS Servers** box, type the IP Address of the Domain Name Servers to be used.

4 If applicable, in the **WINS** box, type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).

Using a DHCP relay for the WM-AD

Although this procedure could also apply to any WM-AD type, normally these settings are defined in the context of DHCP definitions and therefor these values are not available for configurations if DHCP service is not defined.

Using a DHCP relay forces the Summit WM series switch to forward DHCP requests to an external DHCP server on the enterprise network. This function bypasses the local DHCP server for the Summit WM series switch and allows the enterprise to manage IP address allocation to a WM-AD from its existing infrastructure.

The range of IP addresses assigned to the wireless device users on this WM-AD should also be designated on the external DHCP server.

To use an external DHCP server for the WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to use DHCP relay for. The **Topology** tab is displayed.

3 From the **DHCP Option** drop-down list, select **Use DHCP Relay**.

4 In the **Gateway** box, type the IP address for the WM-AD.

5 In the **Mask** box, type the appropriate subnet mask for this IP address.

6 In the **DHCP Server** box, type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this WM-AD. In the case of relay, the Summit WM series switch does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server.

NOTE

The DHCP Server must be configured to match the WM-AD settings. In particular for Routed WM-AD', the DHCP server must identify the Summit WM series switch's interface IP as the default Gateway (router) for the subnet. (Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.)

Configuring topology for a WM-AD for AAA

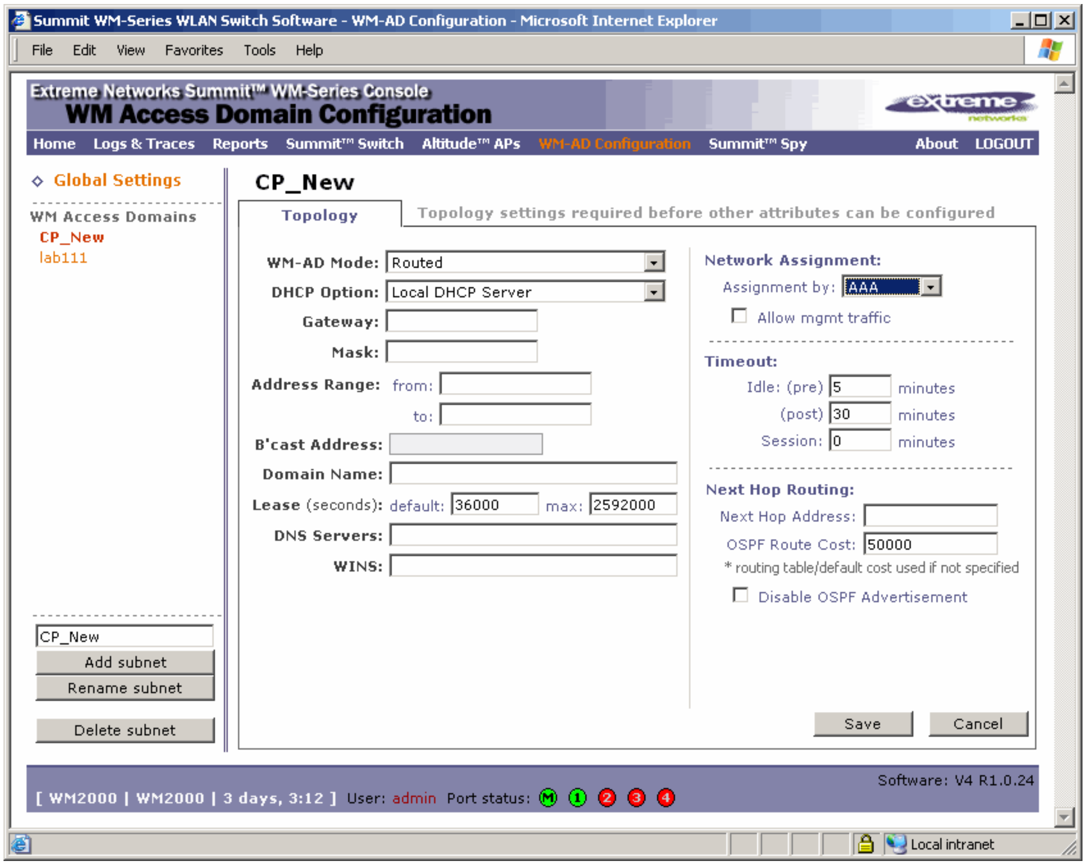
The following sections describe how to configure the topology for a WM-AD for AAA.

To create an AAA topology:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to create an AAA topology for. The **Topology** tab is displayed.

3 From the **Assignment by** drop-down list, select **AAA**.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domains
CP_New
lab111
Add subnet
Rename subnet
Delete subnet
Topology
Save
Cancel
Local intranet

CP_New

Topology settings required before other attributes can be configured

WM-AD Mode: Routed
DHCP Option: Local DHCP Server
Gateway:
Mask:
Address Range: from:
to:
B'cast Address:
Domain Name:
Lease (seconds): default: 36000 max: 2592000
DNS Servers:
WINS:

Network Assignment:
Assignment by: AAA
□ Allow mgmt traffic

Timeout:
Idle: (pre) 5 minutes
(post) 30 minutes
Session: 0 minutes

Next Hop Routing:
Next Hop Address:
OSPF Route Cost: 50000
* routing table/default cost used if not specified
□ Disable OSPF Advertisement

CP_New

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

Software: V4 R1.0.24

4 Configure the topology for your WM-AD accordingly. For more information, see “Topology for a WM-AD” on page 98.

5 To save your changes, click **Save**.

Saving your topology properties

Once your topology is defined, you can then save your topology properties to continue configuring your WM-AD. To save your topology properties, click **Save**.

Assigning Altitude AP radios to a WM-AD

If two Summit WM series switches have been paired for availability (for more information, see “Availability overview” on page 153), each Summit WM series switch's registered Altitude APs will appear as foreign in the list of available Altitude APs on the other Summit WM series switch.

Once you have assigned an Altitude AP radio to eight WM-ADs, it will not appear in the list for another WM-AD setup. Each radio can support up to eight SSIDs (16 per AP). Each AP can be assigned to any of the WM-ADs defined within the system. The following lists the number of WM-ADs that each Summit WM series switch can support:

- WM200 -- up to 32 WM-ADs
- WM2000 -- up to 64 WM-ADs

To assign Altitude APs to a WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to assign Altitude APs to. The **Topology** tab is displayed.

3 Click the **RF** tab.

4 In the **SSID** box, type the SSID that wireless devices will use to access the Altitude AP.

5 In the **Advanced RF Settings**, select the following:

   - **Suppress SSID** – Select to prevent this SSID from appearing in the beacon message sent by the Altitude AP. The wireless device user seeking network access will not see this SSID as an available choice, and will need to specify it.
   - **Enable proprietary IE** – Select to enable radio channel reports to be sent to the Altitude AP for improving roaming time and reliability, as well as improving client power consumption. The AP channel report lists all channels on which the WM-AD can be found—all channels used by all APs that have been assigned to the WM-AD. The AP will provide this list in a proprietary information element to be included in Beacon and Probe response packets. By default this option is disabled. It is recommended to enable this option.
   - **Enable 11h support** – Select to enable TPC (Transmission Power Control) reports. By default this option is disabled. It is recommended to enable this option.
     - **Apply power back-off** – Select to enable the AP to use reduced power (as does the 11h client). By default this option is disabled. It is recommended to enable this option.
   - **Process client IE requests** – Select to enable the AP to accept IE requests sent by clients via Probe Request frames and responds by including the requested IE's in the corresponding Probe Response frames. By default this option is disabled. It is recommended to enable this option.

6 From the **Altitude APs** list, select the APs and their radios that you want to assign to the WM-AD. You can also use the **Select APs** list, to select APs and their radios by grouping:

   - **All radios –** Select to assign all of the APs' radios.
   - **a radios –** Select to assign only the APs' a radios.
   - **b/g radios –** Select to assign only the APs' b/g radios.
   - **local APs** - all radios – Select to assign only the local APs.
   - **local APs** - a radios – Select to assign only the local APs' a radios.
   - **local APs** - b/g radios – Select to assign only the local APs' b/g radios.
   - **foreign APs** - all radios – Select to assign only the foreign APs.
   - **foreign APs** - a radios – Select to assign only the foreign APs' a radios.
   - **foreign APs** - b/g radios – Select to assign only the foreign APs' b/g radios.
   - **clear all selections –** Select to clear all of the AP radio assignments.
   - **original selections –** Select to return to the AP radio selections prior to the most recent save.

7 To save your changes, click **Save**.

You can view the WM-ADs that each radio is assigned to by clicking on each radio tab in the **Altitude AP Configuration** screen.

Authentication for a WM-AD

The next step in configuring a WM-AD is to set up the authentication mechanism. There are various authentication combinations available:

- If network assignment is by SSID, authentication can be:
  - none
  - by Captive Portal using internal Captive Portal
  - by Captive Portal using external Captive Portal
  - by MAC-based authentication
- If network assignment is by AAA (802.1x), authentication can be:
  - by 802.1x authentication, the wireless device user must be authenticated before gaining network access
  - by MAC-based authentication

The first step for any type of authentication is to select RADIUS servers for:

- Authentication
- Accounting
- MAC-based authentication

MAC-based authentication enables network access to be restricted to specific devices by MAC address. In addition to the other types of authentication, when MAC-based authentication is employed the Summit WM series switch queries a RADIUS server to determine if the wireless client's MAC address is authorized to access the network.

Vendor Specific Attributes

In addition to the standard RADIUS message, you can include Vendor Specific Attributes (VSAs). The Summit WM series switch, access points, and WLAN switch software authentication mechanism provides six VSAs for RADIUS and other authentication mechanisms.

Table 4: Vendor Specific Attributes

Attribute Name	ID	Type	Messages	Description
Extreme-URL-Redirection	1	string	Returned from RADIUS server	A URL that can be returned to redirect a session to a specific Web page.
Extreme-AP-Name	2	string	Sent to RADIUS server	The name of the AP the client is associating to. It can be used to assign policy based on AP name or location.
Extreme-AP-Serial	3	string	Sent to RADIUS server	The AP serial number. It can be used instead of (or in addition to) the AP name.

Table 4: Vendor Specific Attributes (Continued)

Attribute Name	ID	Type	Messages	Description
Extreme-WM-AD-Name	4	string	Sent to RADIUS server	The name of the Virtual Network the client has been assigned to. It is used in assigning policy and billing options, based on service selection.
Extreme-SSID	5	string	Sent to RADIUS server	The name of the SSID the client is associating to. It is used in assigning policy and billing options, based on service selection.
Extreme-BSS-MAC	6	string	Sent to RADIUS server	The name of the BSS-ID the client is associating to. It is used in assigning policy and billing options, based on service selection and location.

The first five of these VSAs provide information on the identity of the specific Altitude AP that is handling the wireless device, enabling the provision of location-based services.

The RADIUS message also includes RADIUS attributes Called-Station-Id and Calling-Station-Id in order to include the MAC address of the wireless device.

NOTE

Extreme-URL-Redirection is supported by MAC-based authentication.

Defining authentication for a WM-AD for Captive Portal

For Captive Portal authentication, the wireless device connects to the network, but can only access the specific network destinations defined in the non-authenticated filter. For more information, see "Defining non-authenticated filters" on page 126. One of these destinations should be a server, either internal or external, which presents a Web page login screen—the Captive Portal. The wireless device user must input an ID and a password. This request for authentication is sent by the Summit WM series switch to a RADIUS server or other authentication server. Based on the permissions returned from the authentication server, the Summit WM series switch implements policy and allows the appropriate network access.

Captive Portal authentication relies on a RADIUS server on the enterprise network. There are three mechanisms by which Captive Portal authentication can be carried out:

- **Internal Captive Portal** – The Summit WM series switch presents the Captive Portal Web page, carries out the authentication, and implements policy.
- **External Captive Portal** – After an external server presents the Captive Portal Web page and carries out the authentication, the Summit WM series switch implements policy.
- **External Captive Portal with internal authentication** – After an external server presents the Captive Portal Web page, the Summit WM series switch carries out the authentication and implements policy.

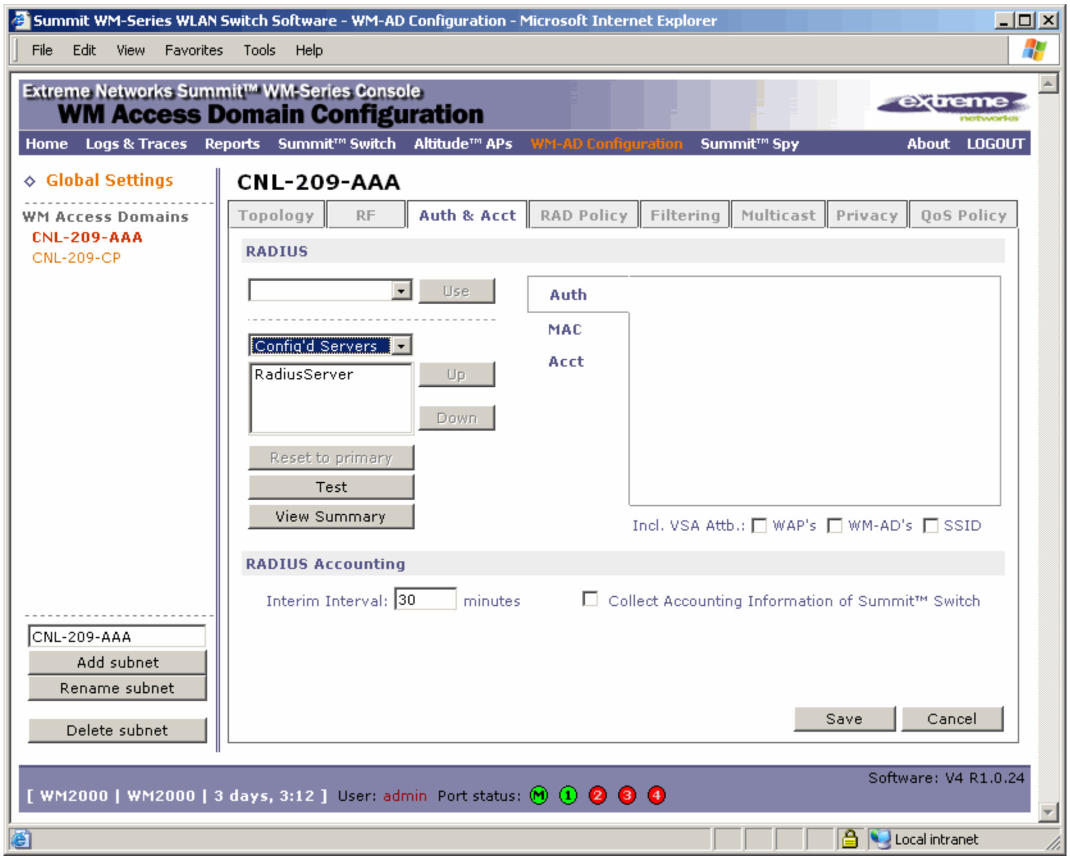
To define authentication by Captive Portal:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to set up authentication by Captive Portal for. The **Topology** tab is displayed.

3 Click the **Auth & Acct** tab. On the **Auth & Acct** tab, there are three options:

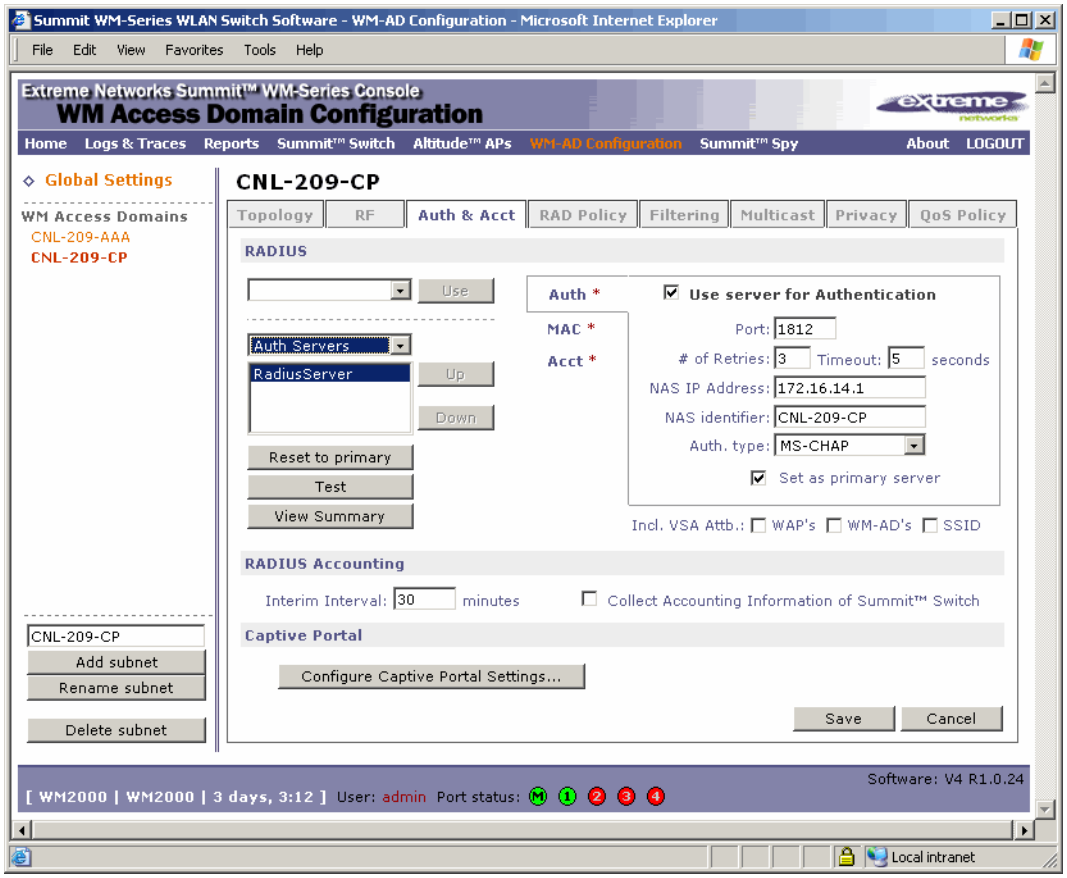
- **Auth** – Use to define authentication servers.
- **MAC** – Use to define servers for MAC-based authentication.
- **Acct** – Use to define accounting servers.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domains
CNL-209-AAA
CNL-209-CP
CNL-209-AAA
Topology RF Auth & Acct RAD Policy Filtering Multicast Privacy QoS Policy
RADIUS
Use
Config'd Servers
RadiusServer
Up
Down
Reset to primary
Test
View Summary
Auth
MAC
Acct
Incl. VSA Attb.: □ WAP's □ WM-AD's □ SSID
RADIUS Accounting
Interim Interval: 30 minutes
□ Collect Accounting Information of Summit™ Switch
CNL-209-AAA
Add subnet
Rename subnet
Delete subnet
Save
Cancel
Software: V4 R1.0.24
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4
Local intranet

4 Click **Auth**. The Authentication fields are displayed.

5 From the **RADIUS** drop-down list, select the server you want to use for Captive Portal authentication, and then click **Use**. The server's default information is displayed.

The RADIUS servers are defined in the Global Settings screen. For more information, see "WM-AD global settings" on page 92.



CNL-209-CP

RADIUS

Auth Servers

RadiusServer

Auth *

MAC *

Acct *

☑ Use server for Authentication

Port: 1812

# of Retries: 3 Timeout: 5 seconds

NAS IP Address: 172.16.14.1

NAS identifier: CNL-209-CP

Auth. type: MS-CHAP

☑ Set as primary server

Incl. VSA Attb.: ☐ WAP's ☐ WM-AD's ☐ SSID

RADIUS Accounting

Interim Interval: 30 minutes ☐ Collect Accounting Information of Summit™ Switch

Captive Portal

CNL-209-CP

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

The selected server is no longer available in the **RADIUS** drop-down list.

The server name is now displayed in the list of configured servers, next to the **Up** and **Down** buttons, where it can be prioritized for RADIUS redundancy. The server can also be assigned again for MAC-based authentication or accounting purposes.

A red asterisk is displayed next to **Auth**, indicating that a server has been assigned.

6 In the **Port** box, type the port used to access the RADIUS server. The default is 1812.

7 In the **# of Retries** box, type the number of times the Summit WM series switch will attempt to access the RADIUS server.

8 In the **Timeout** box, type the maximum time that a Summit WM series switch will wait for a response from the RADIUS server before attempting again.

9 In the **NAS Identifier** box, type the Network Access Server (NAS) identifier. The NAS identifier is a RADIUS attribute that identifies the server responsible for passing information to designated RADIUS servers and then acting on the response returned. This is an optional step.

10 In the **Auth. Type** drop-down list, select the authentication protocol to be used by the RADIUS server to authenticate the wireless device users. The authentication protocol applies to a WM-AD with Captive Portal authentication:

- **PAP** – Password Authentication Protocol
- **CHAP** – Challenge Handshake Authentication Protocol
- **MS-CHAP** – Windows-specific version of CHAP
- **MS-CHAP2** – Windows-specific version of CHAP, version 2

11 In the **Include VSA Attributes** section, click the appropriate checkboxes to include the Vendor Specific Attributes in the message to the RADIUS server:

- **AP's**
- WM-AD's
- **SSID**

The Vendor Specific Attributes must be defined on the RADIUS server.

12 If appropriate, click the **Reset to Primary** checkbox. This checkbox is visible when a RADIUS server has not yet been selected as a primary server, or if the server you are configuring has already been selected as the primary server, the **Reset to Primary** checkbox is selected.

RADIUS redundancy defines additional backup RADIUS servers that the system will attempt to communicate with in case a connection with the identified primary server fails. If connection to an active primary server fails, the system automatically attempts to connect to one of the alternate servers in sequence. If the system succeeds in registering with a defined alternate server, it becomes the active primary server, which is identified by the A on the list. You can subsequently reset or change the identification of the primary server by clicking the applicable **Reset to Primary** checkbox.

13 To save your changes, click **Save**.

NOTE

*If you have already assigned a server to either MAC-based authentication or accounting, and you want to use it again for authentication, highlight its name in the list next to the **Up** and **Down** buttons and select the **Use server for Authentication** checkbox. The server's default information is displayed.*

Defining the RADIUS server priority for RADIUS redundancy

If more than one server has been defined for any type of authentication, you can define the priority of the servers in the case of failover.

In the event of a failover of the main RADIUS server—if there is no response after the set number of retries—then the other servers in the list will be polled on a round-robin basis until a server responds.

If one of the other servers becomes the active server during a failover, when the new active server properties are displayed the **Set as primary server** checkbox is selected.

If all defined RADIUS servers fail to respond, a critical message is generated in the logs.

To define the RADIUS server priority for RADIUS redundancy:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to define the RADIUS server priority for. The **Topology** tab is displayed.

3 Click the **Auth & Acct** tab.

4 From the drop-down list, select the servers group you want to prioritize:

- Configured Servers
- Authentication Servers
- MAC Servers
- Accounting Servers

5 In the server list, select the RADIUS server and click **Up** or **Down** to arrange the order. The first server in the list is the active one.

6 To test the Summit WM series switch's connection to all configured RADIUS servers, click **Test**. The Test RADIUS servers screen displays the message transaction with the RADIUS server, which allows you to visually verify the state of the server connection and user authentication.

The RADIUS test is a test of connectivity to the RADIUS server, not of full RADIUS functionality. AAA WM-ADs use EAP over RADIUS for authentication. The Summit WM series switch's EAP RADIUS connectivity test initiates an Access-Request, to which the RADIUS server will respond with a challenge. If the challenge is received then the test is deemed to have succeeded. If the challenge is not received then the test is deemed to have failed. In either case, the test ends at this point; for AAA WM-ADs, there is no need for a client password below.

7 In the **User ID** box, type the user ID that you know can be authenticated.

8 In the **Password** box, type the corresponding password.

9 Click **Test**. The **Test Result** screen is displayed.

10 To view a summary of the RADIUS configuration, click **View Summary**. The **RADIUS summary** screen is displayed.

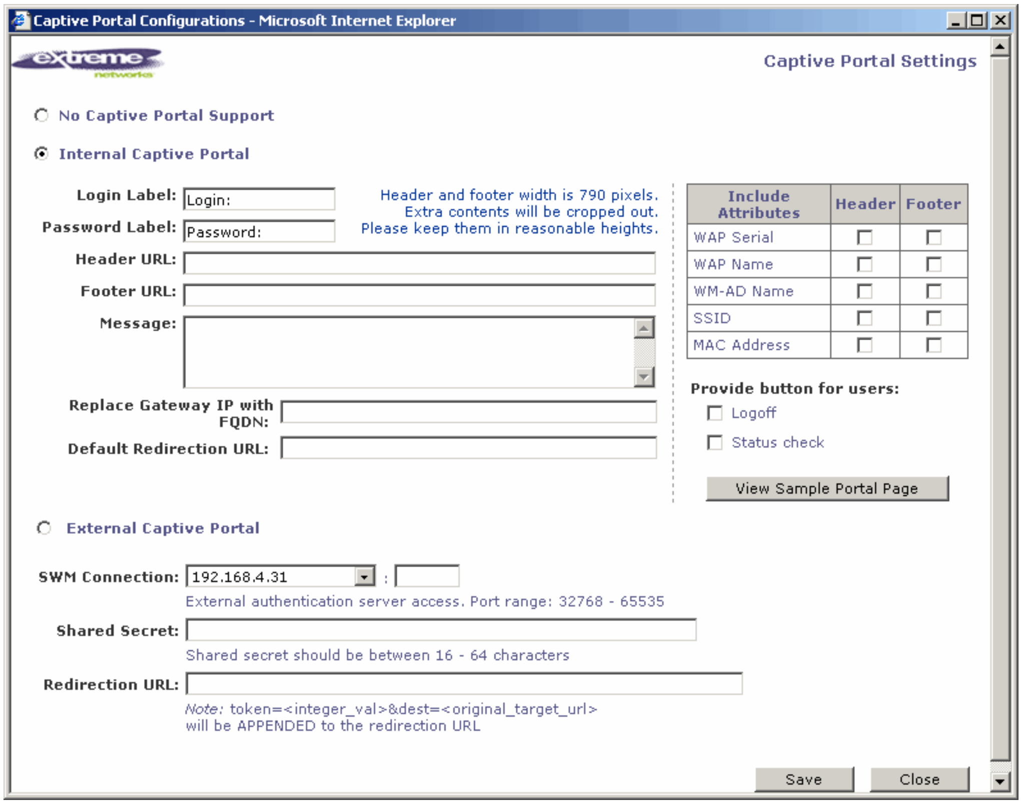
11 To save your changes, click **Save**.

Configuring Captive Portal for internal or external authentication

There are three Captive Portal options:

- No Captive Portal Support
- **Internal Captive Portal** – Define the parameters of the internal Captive Portal page presented by the Summit WM series switch, and the authentication request from the Summit WM series switch to the RADIUS server.
- **External Captive Portal** – Define the parameters of the external Captive Portal page presented by an external server. The authentication can be carried out by an external authentication server or by the Summit WM series switch request to a RADIUS server.

For more information, see "To configure the Captive Portal settings for internal Captive Portal:" on page 114 or "To configure the Captive Portal Settings for external Captive Portal:" on page 115.



Captive Portal Configurations - Microsoft Internet Explorer

Captive Portal Settings

○ No Captive Portal Support

● Internal Captive Portal

Login Label: Login:

Password Label: Password:

Header and footer width is 790 pixels.
Extra contents will be cropped out.
Please keep them in reasonable heights.

Header URL:

Footer URL:

Message:

Replace Gateway IP with FQDN:

Default Redirection URL:

Include Attributes	Header	Footer
WAP Serial	□	□
WAP Name	□	□
WM-AD Name	□	□
SSID	□	□
MAC Address	□	□

Provide button for users:

□ Logoff

□ Status check

View Sample Portal Page

○ External Captive Portal

SWM Connection: 192.168.4.31 :

External authentication server access. Port range: 32768 - 65535

Shared Secret:

Shared secret should be between 16 - 64 characters

Redirection URL:

Note: token=<integer_val>&dest=<original_target_url>
will be APPENDED to the redirection URL

Save Close

To configure the Captive Portal settings for internal Captive Portal:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to configure the Captive Portal settings for. The **Topology** tab is displayed.

3 Click the **Auth & Acct** tab.

4 Click **Configure Captive Portal Settings**. The **Captive Portal Configurations** screen is displayed.

5 Select the **Internal Captive Portal** option.

6 In the **Login Label** box, type the text that will appear as a label for the user login field.

7 In the **Password Label** box, type the text that will appear as a label for the user password field.

8 In the **Header URL** box, type the location of the file to be displayed in the Header portion of the Captive Portal screen. This page can be customized to suit your organization, with logos or other graphics.

WARNING!

If you use logos or graphics, ensure that the graphics or logos are appropriately sized. Large graphics or logos may force the login section out of view.

9 In the **Footer URL** box, type the location of the file to be displayed in the Footer portion of the Captive Portal screen.

10 In the **Message** box, type the message that will appear above the Login box to greet the user. For example, the message could explain why the Captive Portal page is appearing, and instructions for the user.

11 In the **Replace Gateway IP with FQDN** box, type the appropriate name if a Fully Qualified Domain Name (FQDN) is used as the gateway address.

12 In the **Default Redirection URL** box, type the URL to which the wireless device user will be directed to before authentication.

13 In the right pane, select the appropriate checkboxes to include the following VSA Attributes in the message to the authentication server:

- AP Serial number
- AP Name
- WM-AD Name
- SSID
- MAC Address

14 In the right pane, select whether these VSA attributes apply to the header or footer of the Captive Portal page.

The selections influence what URL is returned in either section. For example, wireless users can be identified by which Altitude AP or which WM-AD they are associated with, and can be presented with a Captive Portal Web page that is customized for those identifiers.

15 To provide users with a logoff button, select **Logoff**. The Logoff button launches a pop-up logoff screen, allowing users to control their logoff.

16 To provide users with a status check button, select **Status check**. The Status check button launches a pop-up window, which allows users to monitor session statistics such as system usage and time left in a session.

17 To save your changes, click **Save**.

18 To see how the Captive Portal page you have designed will look, click **View Sample Portal Page**.

NOTE

In order for Captive Portal authentication to be successful, all the URLs referenced in the Captive Portal setup must also be specifically identified and allowed in the non-authenticated filter. For more information, see "Defining non-authenticated filters" on page 126.

To configure the Captive Portal Settings for external Captive Portal:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to configure the Captive Portal settings for. The **Topology** tab is displayed.

3 Click the **Auth & Acct** tab.

4 Click **Configure Captive Portal Settings**. The **Captive Portal Configurations** screen is displayed.

5 Select the **External Captive Portal** option.

6 In the **HWC Connection** drop-down list, select the IP address.

7 Type the port of the Summit WM series switch.

If there is an authentication server configured for this WM-AD, the external Captive Portal page on the external authentication server will send the request back to the Summit WM series switch to allow the Summit WM series switch to continue with the RADIUS authentication and filtering.

In the **Shared Secret** box, type the password common to both the Summit WM series switch and the external Web server if you want to encrypt the information passed between the Summit WM series switch and the external Web server.

8 In the **Redirection URL** box, type the URL to which the wireless device user will be directed to before authentication.

9 To save your changes, click **Save**.

NOTE

You must add a filtering rule to the non-authenticated filter that allows access to the External Captive Portal site. For more information, see "Filtering for a WM-AD" on page 90.

Defining authentication for a WM-AD for AAA

If network assignment is AAA with 802.1x authentication, the wireless device must successfully complete the user authentication verification prior to being granted network access. This enforcement is performed by both the user's client and the AP. The wireless device's client utility must support 802.1x. The user's EAP packets request for network access along with login identification or a user profile is forwarded by the Summit WM series switch to a RADIUS server.

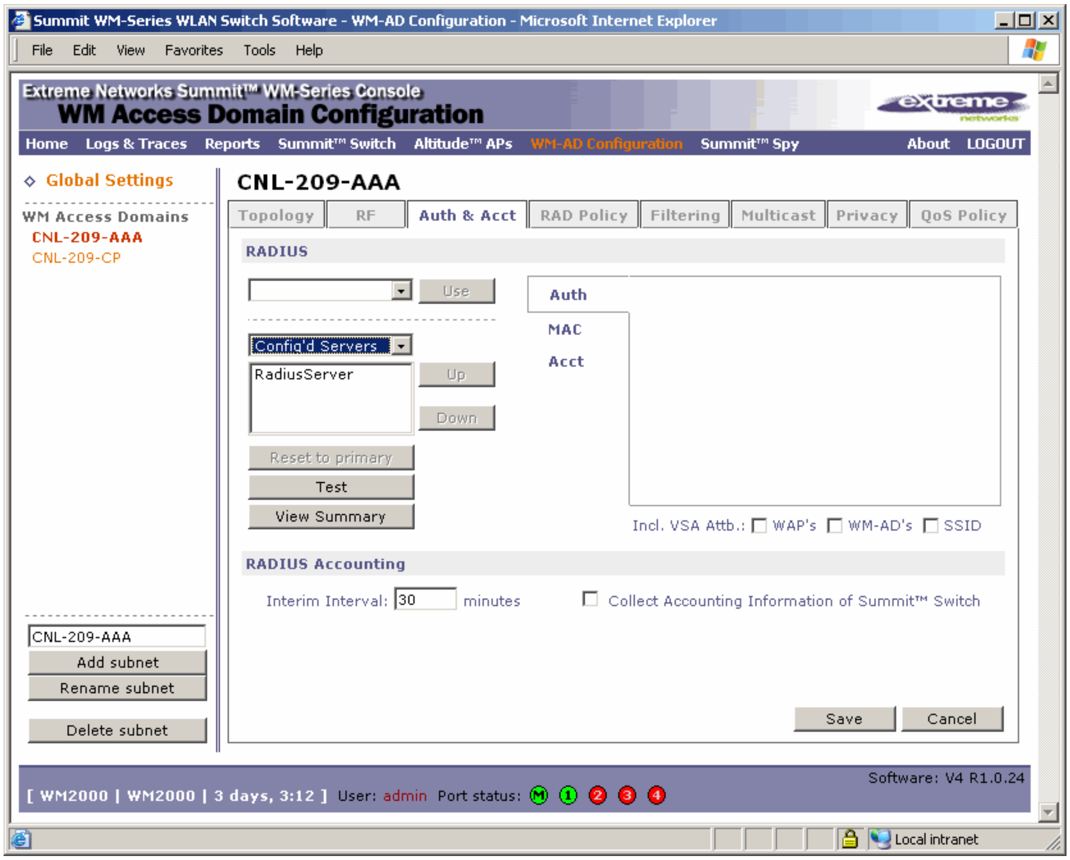
To define authentication by AAA (802.1x):

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to set up authentication by AAA for. The **Topology** tab is displayed.

3 Click the **Auth & Acct** tab. On the **Auth & Acct** tab, there are three options:

- **Auth** – Use to define authentication servers.
- **MAC** – Use to define servers for MAC-based authentication.
- **Acct** – Use to define accounting servers.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer

Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration

CNL-209-AAA

RADIUS

Config'd Servers
RadiusServer

Incl. VSA Attb.: □ WAP's □ WM-AD's □ SSID

RADIUS Accounting

Interim Interval: 30 minutes

□ Collect Accounting Information of Summit™ Switch

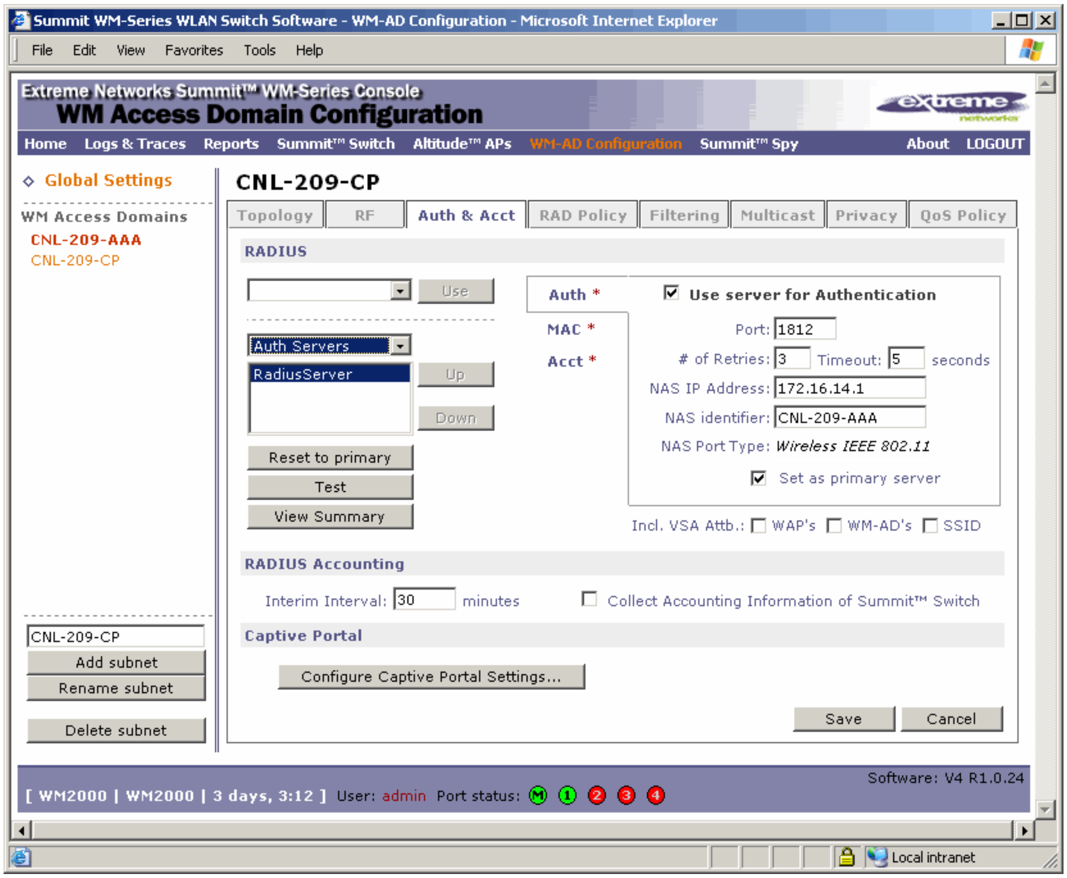
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

Software: V4 R1.0.24

4 Click **Auth**. The Authentication fields are displayed.

5 From the **RADIUS** drop-down list, select the server you want to use for Captive Portal authentication, and then click **Use**. The server's default information is displayed.

The RADIUS servers are defined in the Global Settings screen. For more information, see "WM-AD global settings" on page 92.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domains
CNL-209-AAA
CNL-209-CP
Topology RF Auth & Acct RAD Policy Filtering Multicast Privacy QoS Policy
Use
Up
Down
Reset to primary
Test
View Summary
Add subnet
Rename subnet
Delete subnet
Configure Captive Portal Settings...
Save
Cancel
Local intranet

CNL-209-CP

RADIUS

Auth Servers

RadiusServer

Auth * MAC * Acct *

☑ Use server for Authentication

Port: 1812

# of Retries: 3 Timeout: 5 seconds

NAS IP Address: 172.16.14.1

NAS identifier: CNL-209-AAA

NAS Port Type: *Wireless IEEE 802.11*

☑ Set as primary server

Incl. VSA Attb.: □ WAP's □ WM-AD's □ SSID

RADIUS Accounting

Interim Interval: 30 minutes □ Collect Accounting Information of Summit™ Switch

Captive Portal

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

The selected server is no longer available in the **RADIUS** drop-down list.

The server name is now displayed in the list of configured servers, next to the **Up** and **Down** buttons, where it can be prioritized for RADIUS redundancy. The server can also be assigned again for MAC-based authentication or accounting purposes.

A red asterisk is displayed next to **Auth**, indicating that a server has been assigned.

6 In the **Port** box, type the port used to access the RADIUS server. The default is 1812.

7 In the **# of Retries** box, type the number of times the Summit WM series switch will attempt to access the RADIUS server.

8 In the **Timeout** box, type the maximum time that a Summit WM series switch will wait for a response from the RADIUS server before attempting again.

9 In the **NAS Identifier** box, type the Network Access Server (NAS) identifier. The NAS identifier is a RADIUS attribute that identifies the server responsible for passing information to designated RADIUS servers and then acting on the response returned. This is an optional step.

10 In the **Include VSA Attributes** section, click the appropriate checkboxes to include the Vendor Specific Attributes in the message to the RADIUS server:

- **AP's**
- **WM-AD's**
- **SSID**

The Vendor Specific Attributes must be defined on the RADIUS server.

11 If applicable, select **Set as primary server**.

12 To save your changes, click **Save**.

NOTE

If you have already assigned a server to either MAC-based authentication or accounting, and you want to use it again for authentication, highlight its name in the list next to the ***Up*** *and* ***Down*** *buttons and select the* ***Use server for Authentication*** *checkbox. The server's default information is displayed.*

Defining MAC-based authentication for a WM-AD

MAC-based authentication enables network access to be restricted to specific devices by MAC address. The Summit WM series switch queries a RADIUS server for a MAC address when a wireless client attempts to connect to the network.

MAC-based authentication can be set up on any type of WM-AD, in addition to the Captive Portal or AAA authentication. To set up a RADIUS server for MAC-based authentication, you must set up a user account with UserID=MAC and Password=MAC for each user. Specifying a MAC address format and policy depends on which RADIUS server is being used.

If MAC-based authentication is to be used in conjunction with the 802.1x or Captive Portal authentication, an additional account with a real UserID and Password must also be set up on the RADIUS server.

MAC-based authentication responses may indicate to the Summit WM series switch what WM-AD a user should be assigned to. Authentication (if enabled) can apply on every roam.

To define MAC-based authentication for a WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to set up MAC-based authentication for. The **Topology** tab is displayed.

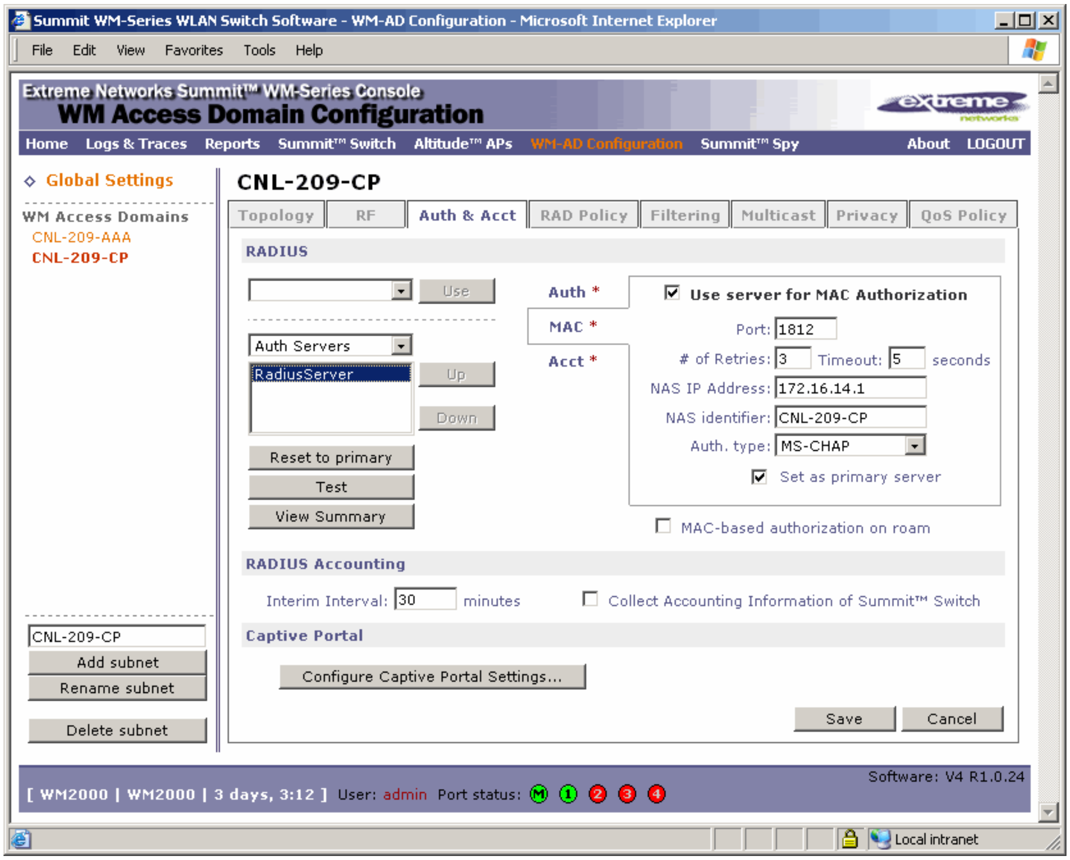
3 Click the **Auth & Acct** tab. On the **Auth & Acct** tab, there are three options:

- **Auth** – Use to define authentication servers.
- **MAC** – Use to define servers for MAC-based authentication.
- **Acct** – Use to define accounting servers.

4 Click **MAC**. The MAC fields are displayed.

5 From the **RADIUS** drop-down list, select the server you want to use for MAC authentication, and then click **Use**. The server’s default information is displayed and a red asterisk is displayed next to **MAC**, indicating that a server has been assigned.

The RADIUS servers are defined in the Global Settings screen. For more information, see “WM-AD global settings” on page 92.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domains
CNL-209-AAA
CNL-209-CP
Topology RF Auth & Acct RAD Policy Filtering Multicast Privacy QoS Policy
Use
Up
Down
Reset to primary
Test
View Summary
Auth *
MAC *
Acct *
Add subnet
Rename subnet
Delete subnet
Configure Captive Portal Settings...
Save
Cancel
Local intranet

CNL-209-CP

RADIUS

Auth Servers: RadiusServer

☑ Use server for MAC Authorization

Port: 1812

# of Retries: 3 Timeout: 5 seconds

NAS IP Address: 172.16.14.1

NAS identifier: CNL-209-CP

Auth. type: MS-CHAP

☑ Set as primary server

☐ MAC-based authorization on roam

RADIUS Accounting

Interim Interval: 30 minutes ☐ Collect Accounting Information of Summit™ Switch

Captive Portal

CNL-209-CP

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

6 If applicable, to use a server that has already been used for another type of authentication or accounting, select the server you want to use for MAC authentication, and then select **User server for MAC Authentication**.

7 In the **Port** box, type the port used to access the RADIUS server. The default is 1812.

8 In the **# of Retries** box, type the number of times the Summit WM series switch will attempt to access the RADIUS server.

9 In the **Timeout** box, type the maximum time, in seconds, that a Summit WM series switch will wait for a response from the RADIUS server before attempting again.

10 In the **NAS IP Address** box, type the Network Access Server (NAS) IP address.

11 In the **NAS Identifier** box, type the Network Access Server (NAS) identifier. The NAS identifier is a RADIUS attribute that identifies the server responsible for passing information to designated RADIUS servers and then acting on the response returned. This is an optional step.

12 In the **Auth. Type** field, select the authentication protocol to be used by the RADIUS server to authenticate the wireless device users for a Captive Portal WM-AD.

13 In the **Include VSA Attributes** section, click the appropriate checkboxes to include the Vendor Specific Attributes in the message to the RADIUS server:

- **AP's**
- **WM-AD's**
- **SSID**

The Vendor Specific Attributes must be defined on the RADIUS server.

14 If applicable, select **Set as primary server**.

15 To enable MAC-based authentication on roam, select the **MAC-based authentication on roam** checkbox.

NOTE

Only select this checkbox if you are using MAC based authentication and if you want your clients to be authorized every time they roam to another AP. If this feature is not enabled, and MAC-based authentication is in use, the client is authenticated only at the start of a session.

16 To save your changes, click **Save**.

Defining accounting methods for a WM-AD

The next step in configuring a WM-AD is to define the methods of accounting. Accounting tracks the activity of a wireless device users. There are two types of accounting available:

- **Summit WM series switch accounting** – Enables the Summit WM series switch to generate Call Data Records (CDRs) in a flat file on the Summit WM series switch.
- **RADIUS accounting** – Enables the Summit WM series switch to generate an accounting request packet with an accounting start record after successful login by the wireless device user, and an accounting stop record based on session termination. The Summit WM series switch sends the accounting requests to a remote RADIUS server.

Summit WM series switch accounting creates Call Data Records (CDRs) in a standard format of authenticated user sessions, such as start time and duration of session. The CDRs are stored in flat files that can be downloaded via the Command Line Interface (CLI).

If RADIUS accounting is enabled, a RADIUS accounting server needs to be specified.

To define accounting methods for a WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to define accounting methods for. The **Topology** tab is displayed.

3 Click the **Auth & Acct** tab.

4 To enable Summit WM series switch accounting, select **Collect Accounting Information of Wireless Controller**.

5 From the **RADIUS** drop-down list, select the server you want to use for RADIUS accounting, and then click **Use**. The server's default information is displayed and a red asterisk is displayed next to **Acct**, indicating that a server has been assigned.

   The RADIUS servers are defined in the Global Settings screen. For more information, see "WM-AD global settings" on page 92.

6 Select **Use server for RADIUS Accounting**.

7 In the **Port** box, type the port used to access the RADIUS server. The default is 1812.

8 In the **# of Retries** box, type the number of times the Summit WM series switch will attempt to access the RADIUS server.

9 In the **Timeout** box, type the maximum time that a Summit WM series switch will wait for a response from the RADIUS server before attempting again.

10 In the **Interim Interval** box, type the time interval when accounting records are sent. Interim accounting records are sent if the interim time interval is reached before the session ends. The default is 60 minutes.

11 To save your changes, click **Save**.

Defining RADIUS filter policy for WM-ADs and WM-AD groups

The next step in configuring a WM-AD is to define the filter ID values for a WM-AD. These filter ID values must match those set up on the RADIUS servers.

NOTE

This configuration step is optional. If filter ID values are not defined, the system uses the default filter as the applicable filter group for authenticated users within a WM-AD. However, if more user-specific filter definitions are required, for example filters based on a user's department, then the filter ID configuration is used to overwrite the default assignment.

In addition to the filter ID values, you can also set up a group ID for a WM-AD with AAA authentication. You can set up a group within a WM-AD that relies on the RADIUS attribute Login-LAT-Group (RFC2865). For each group, you can define filtering rules to control access to the network.

If you define a group within an AAA WM-AD, the group (or child) definition acquires the same authentication and privacy parameters as the parent WM-AD. However, you need to define a different topology and filtering rules for this group.

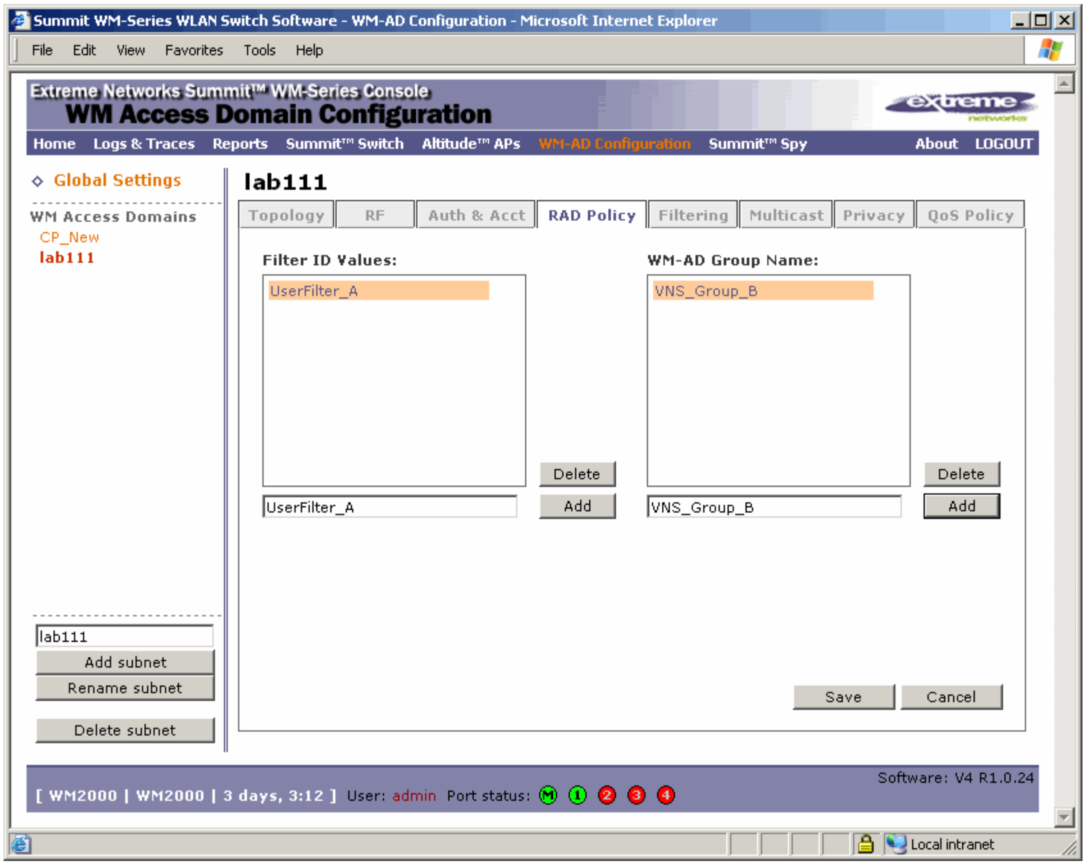
All the filters are exposed. For the Assignment by SSID with no authentication, the filter that is applied to the client session is the default filter.

To define the filter ID values on a WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to define filter ID values for. The **Topology** tab is displayed.

3 Click the **RAD Policy** tab.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domains
CP_New
lab111
lab111
Topology RF Auth & Acct RAD Policy Filtering Multicast Privacy QoS Policy
Delete
Add
Delete
Add
Add subnet
Rename subnet
Delete subnet
Save
Cancel
Port status:
Local intranet

Filter ID Values: UserFilter_A

WM-AD Group Name: VNS_Group_B

[WM2000 | WM2000 | 3 days, 3:12] User: admin

Software: V4 R1.0.24

4 In the **Filter ID Values** box, type the name of a group that you want to define specific filtering rules for to control network access.

5 Click the corresponding **Add** button. The filter ID value is displayed in the list. These filter ID values will appear in the **Filter ID** list on the **Filtering** tab. These filter ID values must match those set up for the filter ID attribute in the RADIUS server.

6 If applicable, repeat steps 4 and 5 to add additional filtering ID values.

7 In the **WM-AD Group Name** box, type the name of a WM-AD group you want to create and define within the selected parent WM-AD.

8 Click the corresponding **Add** button. The Group Name will appear as a child of the parent WM-AD in the left pane **WM Access Domains** list.

9 To your changes, click **Save**.

Configuring filtering rules for a WM-AD

The next step in configuring a WM-AD is to configure the filtering rules for a WM-AD.

In an AAA WM-AD, a non-authenticated filter is unnecessary because users have already been authenticated. When authentication is returned, the filter ID group filters are applied. For AAA, a WM-AD can have a sub-group with Login-LAT-group ID that has its own filtering rules. If no filter ID matches are found, then the default filter is applied. WM-AD Policy is also applicable for Captive Portal and MAC-based authorization.

Filtering rules for an exception filter

The exception filter provides a set of rules aimed at restricting the type of traffic that is delivered to the controller. By default, your system is shipped with a set of restrictive filtering rules that help control access through the interfaces to only absolutely necessary services.

By configuring to allow management on an interface, an additional set of rules is added to the shipped filter rules that provide access to the system's management configuration framework (SSH, HTTPS, SNMPAgent). Most of this functionality is handled directly behind the scenes by the system, rolling and un-rolling canned filters as the system's topology and defined access privileges for an interface change.

NOTE

*An interface for which **Allow Management** is enabled, can be reached by any other interface. By default, **Allow Management** is disabled and shipped interface filters will only permit the interface to be visible directly from it's own subnet.*

The visible exception filters definitions, both in physical ports and WM-AD definitions, allow administrators to define a set of rules to be prepended to the system's dynamically updated exception filter protection rules. Rule evaluation is performed top to bottom, until an exact match is determined. Therefor, these user-defined rules are evaluated before the system's own generated rules. As such, these user-defined rules may inadvertently create security lapses in the system's protection mechanism or create a scenario that filters out packets that are required by the system.

NOTE

Use exception filters only if absolutely necessary. It is recommended to avoid defining general allow all or deny all rule definitions since those definitions can easily be too liberal or too restrictive to all types of traffic.

The exception rules are evaluated in the context of referring to the specific controller's interface. The destination address for the filter rule definition is typically defined as the interface's own IP address. The port number for the filter definition corresponds to the target (destination) port number for the applicable service running on the controller's management plane.

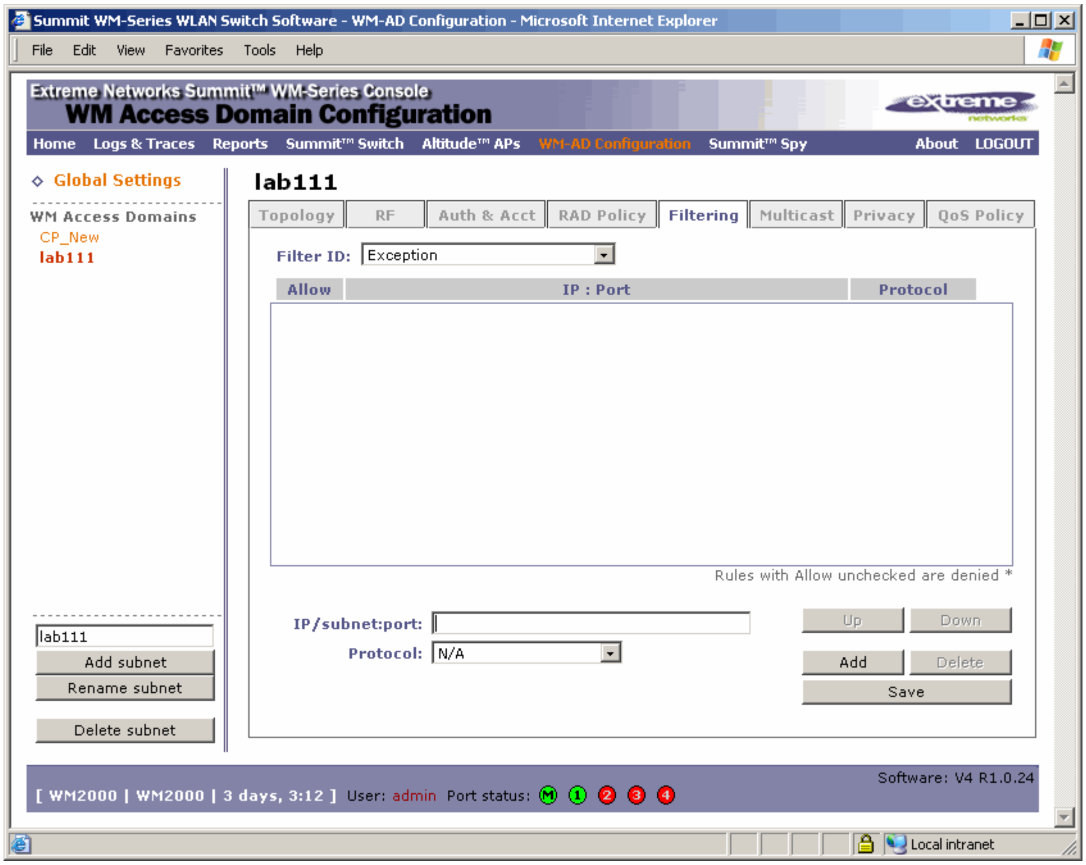
The exception filter on an WM-AD applies only to the destination portion of the packet. Traffic to a specified IP address and IP port is either allowed or denied. Adding exception filtering rules allows network administrators to either tighten or relax the built-in filtering that automatically drops packets not specifically allowed by filtering rule definitions. The exception filtering rules can deny access in the event of a DoS attack, or can allow certain types of management traffic that would otherwise be denied. Typically, **Allow Management** is enabled

To define filtering rules for an exception filter:

1. From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.
2. In the left pane **WM Access Domains** list, click the WM-AD you want to define filter ID values for. The **Topology** tab is displayed.

3 Click the **Filtering** tab.

4 From the **Filter ID** drop-down list, select **Exception**.



Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer

Extreme Networks Summit™ WM-Series Console

WM Access Domain Configuration

lab111

Filter ID: Exception

Rules with Allow unchecked are denied *

IP/subnet:port:

Protocol: N/A

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

Software: V4 R1.0.24

5 For each filtering rule you are defining, do the following:

- In the **IP/subnet:port** box, type the destination IP address. You can also specify an IP range, a port designation, or a port range on that IP address.
- In the **Protocol** drop-down list, select the applicable protocol. The default is N/A.

6 Define a rule to allow access to the default gateway for this WM-AD:

- Select **IP/Port.**
- Type the default gateway IP address (WM-AD's IP address) that you defined in the **Topology** tab for this WM-AD.

7 Click **Add**. The information is displayed in the **Filter Rules** section of the tab.

8 Select the new filter, then select the **Allow** checkbox applicable to the rule you defined.

9 Edit the order of a filter by selecting the filter and clicking the **Up** and **Down** buttons. The filtering rules are executed in the order you define here.

10 To save your changes, click **Save**.

NOTE

For external Captive Portal, you need to add an external server to a non-authentication filter.

Defining non-authenticated filters

Defining non-authenticated filters allows administrators to identify destinations to which a user is allowed to access without incurring an authentication redirection. Typically, the recommended default rule is to deny all. Administrators should define a rule set that will permit users to access essential services:

- DNS (IP of DNS server)
- Default Gateway (WM-AD Interface IP)

Any HTTP streams requested by the client for denied targets will be redirected to the specified location.

The non-authenticated filter should allow access to the Captive Portal page IP address, as well as to any URLs for the header and footer of the Captive Portal page. This filter should also allow network access to the IP address of the DNS server and to the network address—the gateway of the WM-AD. The WM-AD gateway is used as the IP for an internal Captive Portal page. An external Captive Portal will provide a specific IP definition of a server outside the Summit WM series switch.

Redirection and Captive Portal credentials apply to HTTP traffic only. A wireless device user attempting to reach Websites other than those specifically allowed in the non-authenticated filter will be redirected to the allowed destinations. Most HTTP traffic outside of those defined in the non-authenticated filter will be redirected.

NOTE

Although non-authenticated filters definitions are used to assist in the redirection of HTTP traffic for restricted or denied destinations, the non-authenticated filter is not restricted to HTTP operations. The filter definition is general. Any traffic other than HTTP that the filter does not explicitly allow will be discarded by the controller.

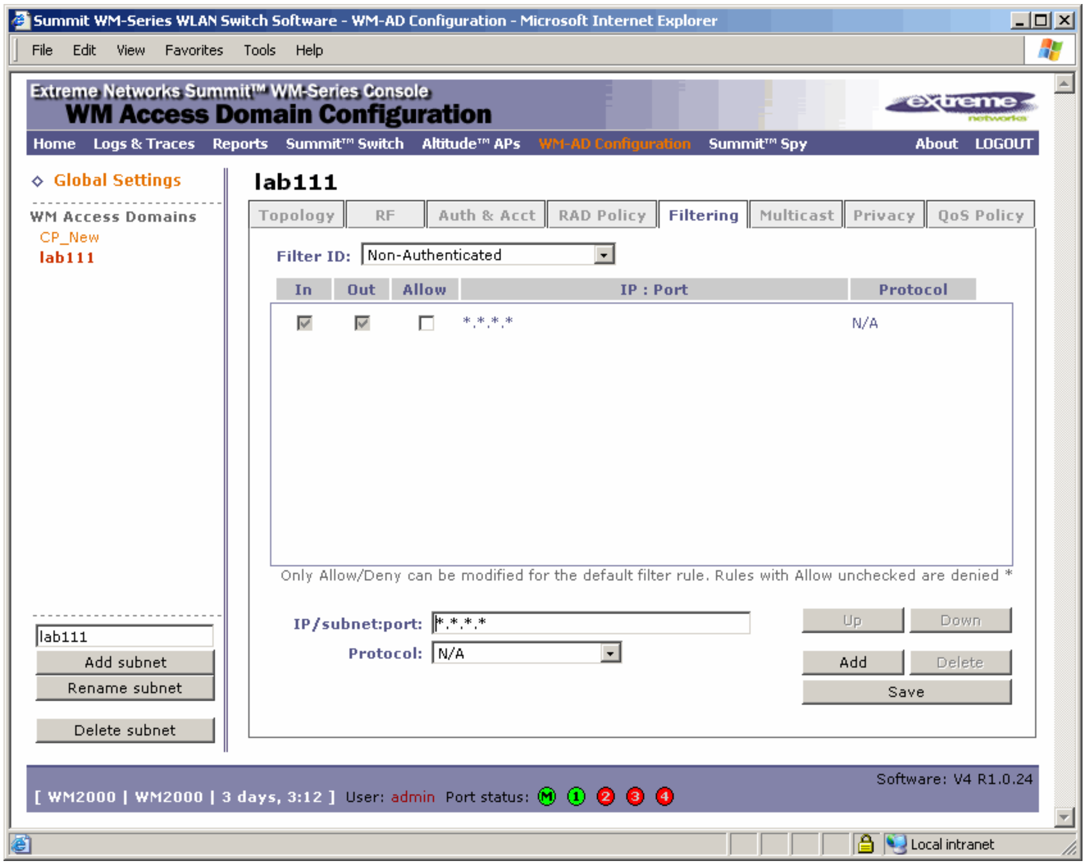
The non-authenticated filter is applied by the Summit WM series switch to sessions until they successfully complete authentication. The authentication procedure results in an adjustment to the user's applicable filters for access policy. The authentication procedure may result in the specification of a specific filter ID or the application of the default filter for the WM-AD.

Typically, default filter ID access is less restrictive than a non-authenticated profile. It is the administrator’s responsibility to define the correct set of access privileges.

To define filtering rules for a non-authenticated filter:

1. From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.
2. In the left pane **WM Access Domains** list, click the WM-AD you want to define filter ID values for. The **Topology** tab is displayed.
3. Click the **Filtering** tab.

4 From the **Filter ID** drop-down list, select **Non-Authenticated**.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domains
CP_New
lab111
Add subnet
Rename subnet
Delete subnet
Topology RF Auth & Acct RAD Policy Filtering Multicast Privacy QoS Policy
Up Down Add Delete Save
Local intranet

lab111

Filter ID: Non-Authenticated

In	Out	Allow	IP : Port	Protocol
☑	☑	□	*.*.*.*	N/A

Only Allow/Deny can be modified for the default filter rule. Rules with Allow unchecked are denied *

IP/subnet:port: *.*.*.*

Protocol: N/A

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

The **Filtering** tab automatically provides a Deny All rule already in place. Use this rule as the final rule in the non-authenticated filter for Captive Portal.

5 For each filtering rule you are defining, do the following:

- In the **IP/subnet:port** box, type the destination IP address. You can also specify an IP range, a port designation, or a port range on that IP address.
- In the **Protocol** drop-down list, select the applicable protocol. The default is N/A.

6 For Captive Portal assignment, define a rule to allow access to the default gateway for this WM-AD:

- Select **IP/Port.**
- Type the default gateway IP address that you defined in the **Topology** tab for this WM-AD.

7 Click **Add**. The information is displayed in the **Filter Rules** section of the tab.

8 Select the new filter, then do the following:

- If applicable, select **In** to refer to traffic from the wireless device that is trying to get on the network.
- If applicable, select **Out** to refer to traffic from the network host that is trying to get to a wireless device.
- Select the **Allow** checkbox applicable to the rule you defined.

9 Edit the order of a filter by selecting the filter and clicking the **Up** and **Down** buttons. The filtering rules are executed in the order you define here.

10 To save your changes, click **Save**.

NOTE

Administrators must ensure that the non-authenticated filter allows access to the corresponding authentication server:

- **Internal Captive Portal** – IP address of the WM-AD interface
- **External Captive Portal** – IP address of external Captive Portal server

Non-authenticated filter examples

A basic non-authenticated filter for internal Captive Portal should have three rules, in the following order:

Table 5: Non-authenticated filter example A

In	Out	Allow	IP / Port	Description
x	x	x	IP address of default gateway (WM-AD Interface IP)	Allow all incoming wireless devices access to the default gateway of the WM-AD.
x	x	x	IP address of the DNS Server	Allow all incoming wireless devices access to the DNS server of the WM-AD.
x	x		*.*.*.*	Deny everything else.

NOTE

For external Captive Portal, an additional rule to Allow (in/out) access to the external Captive Portal authentication/ Web server is required.

If you place URLs in the header and footer of the Captive Portal page, you must explicitly allow access to any URLs mentioned in the authentication's server page, such as:

- **Internal Captive Portal** – URLs referenced in a header or footer
- **External Captive Portal** – URLs mentioned in the page definition

Here is another example of a non-authenticated filter that adds two more filtering rules. The two additional rules do the following:

- Deny access to a specific IP address.
- Allows only HTTP traffic.

Table 6: Non-authenticated filter example B

In	Out	Allow	IP / Port	Description
x	x	x	IP address of the default gateway	Allow all incoming wireless devices access to the default gateway of the WM-AD.
x	x	x	IP address of the DNS Server	Allow all incoming wireless devices access to the DNS server of the WM-AD.
x	x		[a specific IP address, or address plus range]	Deny all traffic to a specific IP address, or to a specific IP address range (such as:0/24).
x	x		*.*.*.*:80	Deny all port 80 (HTTP) traffic.
x	x		*.*.*.*	Deny everything else.

Once a wireless device user has logged in on the Captive Portal page, and has been authenticated by the RADIUS server, then the following filters will apply:

- **Filter ID** – If a filter ID associated with this user was returned by the authentication server.
- **Default filter** – If no matching filter ID was returned from the authentication server

Filtering rules for a filter ID group

When the wireless device user provides the identification credentials, identification is sent by the Summit WM series switch to the RADIUS server, or other authentication server, through a sequence of exchanges depending on the type of authentication protocol used.

When the server allows this request for authentication—the server sends an access-accept message, the RADIUS server may also send back to the Summit WM series switch a filter ID attribute value associated with the user. For an AAA WM-AD, a Login-LAT-Group identifier for the user may also be returned. WM-AD Policy is also applicable for Captive Portal and MAC-based authorization.

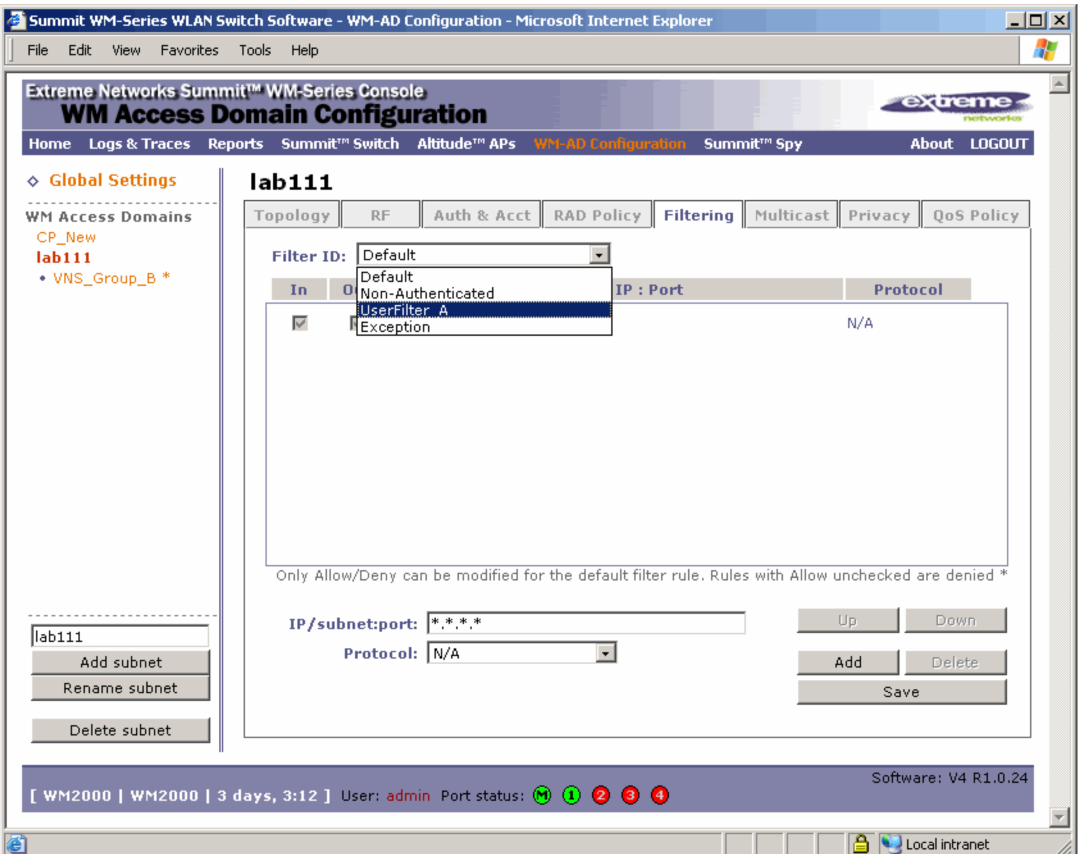
If the filter ID attribute value (or Login-LAT-Group attribute value) from the RADIUS server matches a filter ID value that you have set up on the Summit WM series switch, the Summit WM series switch applies the filtering rules that you defined for that filter ID value to the wireless device user.

If no filter ID is returned by the authentication server, or no match is found on the Summit WM series switch, the filtering rules in the default filter will apply to the wireless device user.

To define filtering rules for a filter ID group:

1. From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.
2. In the left pane **WM Access Domains** list, click the WM-AD you want to define filtering rules for a filter ID group. The **Topology** tab is displayed.
3. Click the **Filtering** tab.

4 From the **Filter ID** drop-down list, select one of the names you defined in the **Filter ID Values** field on the **RAD Policy** tab. For example, select one of your organization's user groups, such as Sales, Engineering, Teacher, Guest, etc.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domains
CP_New
lab111
VNS_Group_B *
lab111
Topology RF Auth & Acct RAD Policy Filtering Multicast Privacy QoS Policy
In Out IP : Port Protocol
Up Down Add Delete Save
Add subnet Rename subnet Delete subnet
Local intranet

Filter ID: Default

Default
Non-Authenticated
UserFilter_A
Exception

N/A

Only Allow/Deny can be modified for the default filter rule. Rules with Allow unchecked are denied *

IP/subnet:port: *.*.*.*

Protocol: N/A

lab111

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

The **Filtering** tab automatically provides a Deny All rule already in place. This rule can be modified to Allow All, if appropriate to the network access needs for this WM-AD.

5 For each filtering rule you are defining, do the following:

- In the **IP/subnet:port** box, type the destination IP address. You can also specify an IP range, a port designation, or a port range on that IP address.
- In the **Protocol** drop-down list, select the applicable protocol. The default is N/A.

6 Click **Add**. The information is displayed in the **Filter Rules** section of the tab.

7 Select the new filter, then do the following:

- If applicable, select **In** to refer to traffic from the wireless device that is trying to get on the network.
- If applicable, select **Out** to refer to traffic from the network host that is trying to get to a wireless device.
- Select the **Allow** checkbox applicable to the rule you defined.

8 Edit the order of a filter by selecting the filter and clicking the **Up** and **Down** buttons. The filtering rules are executed in the order you define here.

9 To save your changes, click **Save**.

Filtering rules by filter ID examples

Below are two examples of possible filtering rules for a filter ID. The first example disallows some specific access before allowing everything else.

Table 7: Filtering rules by filter ID example A

In	Out	Allow	IP / Port	Description
x	x		*.*.*.*:22-23	SSH and telnet sessions
x	x		[specific IP address, range]	Deny all traffic to a specific IP address or address range
x	x	x	*.*.*.*.	Allow everything else

The second example does the opposite of the first example. It allows some specific access and denies everything else.

Table 8: Filtering rules by filter ID example B

In	Out	Allow	IP / Port	Description
x	x	x	[specific IP address, range]	Allow traffic to a specific IP address or address range.
x	x		*.*.*.*.	Deny everything else.

Filtering rules for a default filter

After authentication of the wireless device user, the default filter will apply only after:

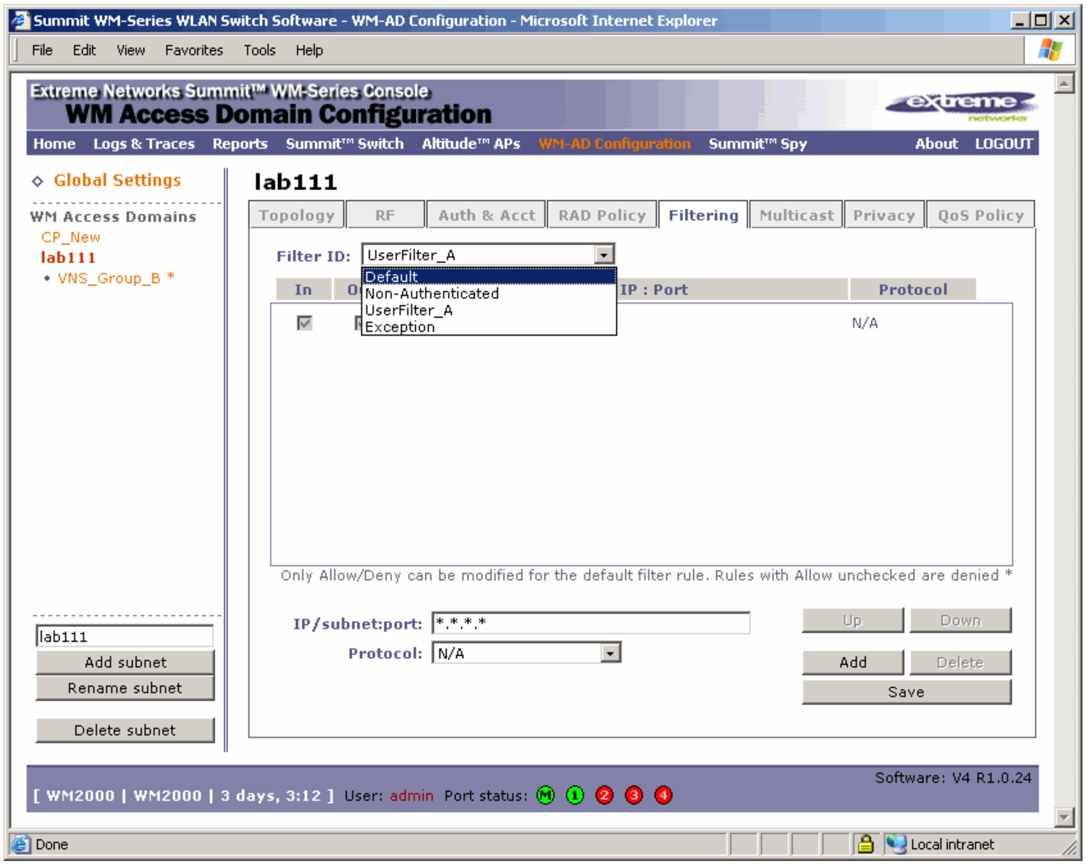
- No match is found for the Exception filter rules.
- No filter ID attribute value is returned by the authentication server for this user.
- No match is found on the Summit WM series switch for a filter ID value.

The final rule in the default filter should be a catch-all rule for any traffic that did not match a filter. A final Allow All rule in a default filter will ensure that a packet is not dropped entirely if no other match can be found. WM-AD Policy is also applicable for Captive Portal and MAC-based authorization.

To define the filtering rules for a default filter:

1. From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.
2. In the left pane **WM Access Domains** list, click the WM-AD you want to define the filtering rules for a default filter. The **Topology** tab is displayed.
3. Click the **Filtering** tab.

4 From the **Filter ID** drop-down list, select **Default**.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domains
CP_New
lab111
VNS_Group_B *
lab111
Topology RF Auth & Acct RAD Policy Filtering Multicast Privacy QoS Policy
In
O
IP : Port
Protocol
N/A
Up
Down
Add
Delete
Save
lab111
Add subnet
Rename subnet
Delete subnet
Done
Local intranet

Filter ID: UserFilter_A

- Default
- Non-Authenticated
- UserFilter_A
- Exception

Only Allow/Deny can be modified for the default filter rule. Rules with Allow unchecked are denied *

IP/subnet:port: *.*.*.*

Protocol: N/A

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

The **Filtering** tab automatically provides a Deny All rule already in place. This rule can be modified to Allow All, if appropriate to the network access needs for this WM-AD.

Default filter examples

The following are examples of filtering rules for a default filter:

Table 9: Default filter example A

In	Out	Allow	IP / Port	Description
x	x		Intranet IP, range	Deny all access to an IP range
x	x		Port 80 (HTTP)	Deny all access to Web browsing
x	x		Intranet IP	Deny all access to a specific IP
x	x	x	*.*.*.*.	Allow everything else

Table 10: Default filter example B

In	Out	Allow	IP / Port	Description
x			Port 80 (HTTP) on host IP	Deny all incoming wireless devices access to Web browsing the host
	x		Intranet IP 10.3.0.20, ports 10-30	Deny all traffic from the network to the wireless devices on the port range, such as TELNET (port 23) or FTP (port 21)

Table 10: Default filter example B (Continued)

In	Out	Allow	IP / Port	Description
x		x	Intranet IP 10.3.0.20	Allow all other traffic from the wireless devices to the Intranet network
	x	x	Intranet IP 10.3.0.20	Allow all other traffic from Intranet network to wireless devices
x	x	x	*.*.*.*.	Allow everything else

Filtering rules for an AAA child group WM-AD

If you defined a child group for an AAA WM-AD, it will have the same authentication parameters and filter IDs as the parent WM-AD. However, you can define different filtering rules for the filters IDs in the child configuration from those in the parent configuration.

Filtering rules between two wireless devices

Traffic from two wireless devices that are on the same WM-AD and are connected to the same Altitude AP will pass through the Summit WM series switch and therefore be subject to filtering policy. You can set up filtering rules that allow each wireless device access to the default gateway, but also prevent each device from communicating with each other.

Add the following two rules to a filter ID filter, before allowing everything else:

Table 11: Rules between two wireless devices

In	Out	Allow	IP / Port	Description
x	x	x	[Intranet IP]	Allow access to the Gateway IP address of the WM-AD only
x	x		[Intranet IP, range]	Deny all access to the WM-AD subnet range (such as 0/24)
x	x	x	*.*.*.*.	Allow everything else

Enabling multicast for a WM-AD

A mechanism that supports multicast traffic can be enabled as part of a WM-AD definition. This mechanism is provided to support the demands of VoIP and IPTV network traffic, while still providing the network access control.

Define a list of multicast groups whose traffic is allowed to be forwarded to and from the WM-AD. The default behavior is to drop the packets. For each group defined, you can enable Multicast Replication by group.

NOTE

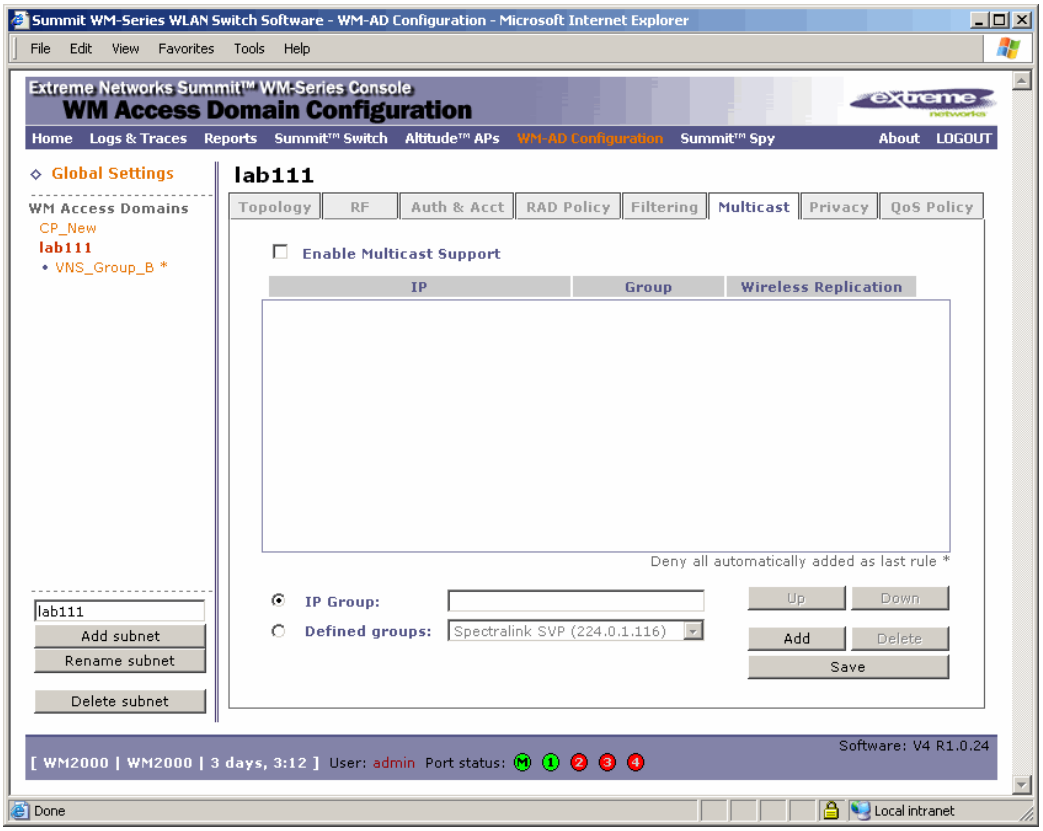
*Before enabling multicast filters and depending on the topology of the WM-AD, you may need to define which physical interface to use for multicast relay. Define the multicast port on the **IP Addresses** screen. For more information, see "Setting up the data ports" on page 42.*

To enable multicast for a WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to enable Multicast for. The **Topology** tab is displayed.

3 Click the **Multicast** tab.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domains
CP_New
lab111
• VNS_Group_B *
lab111
Topology RF Auth & Acct RAD Policy Filtering Multicast Privacy QoS Policy
Enable Multicast Support
IP Group Wireless Replication
Deny all automatically added as last rule *
IP Group:
Defined groups:
Up Down
Add Delete
Save
Add subnet
Rename subnet
Delete subnet
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4
Software: V4 R1.0.24
Done
Local intranet

☐ Enable Multicast Support

○ IP Group:

○ Defined groups: Spectralink SVP (224.0.1.116)

lab111

4 To enable the multicast function, click **Enable Multicast Support**.

5 Define the multicast groups by selecting one of the radio buttons:

- **IP Group** – Type the IP address range.
- **Defined groups** – Select from the drop-down list.

6 Click **Add**. The group is added to the list above.

7 To enable the wireless multicast replication for this group, select the corresponding **Wireless Replication** checkbox.

8 To modify the priority of the multicast groups, select the group row and click the **Up** or **Down** buttons.

A Deny All rule is automatically added as the last rule, IP = *.*.*.* and the **Wireless Replication** checkbox is not selected. This rule ensures that all other traffic is dropped.

9 To save your changes, click **Save**.

NOTE

The multicast packet size should not exceed 1450 bytes.

Configuring privacy for a WM-AD

Privacy is a mechanism that protects data over wireless and wired networks, usually by encryption techniques. The following section describes how the Privacy mechanism is handled for a Captive Portal WM-AD and an AAA WM-AD.

Privacy for a WM-AD for Captive Portal

For the Captive Portal WM-AD, there are three options for the privacy mechanism:

- None
- **Static Wired Equivalent Privacy (WEP)** – Keys for a selected WM-AD, so that it matches the WEP mechanism used on the rest of the network. Each radio can support up to eight SSIDs (16 per AP). Each AP can participate in up to 50 WM-ADs. For each WM-AD, only one WEP key can be specified. It is treated as the first key in a list of WEP keys.
- **Wi-Fi Protected Access (WPA) Pre-Shared key (PSK)** – Privacy in PSK mode, using a Pre-Shared Key (PSK), or shared secret for authentication. WPA-PSK is a security solution that adds authentication to enhanced WEP encryption and key management. WPA-PSK mode does not require an authentication server. It is suitable for home or small office.

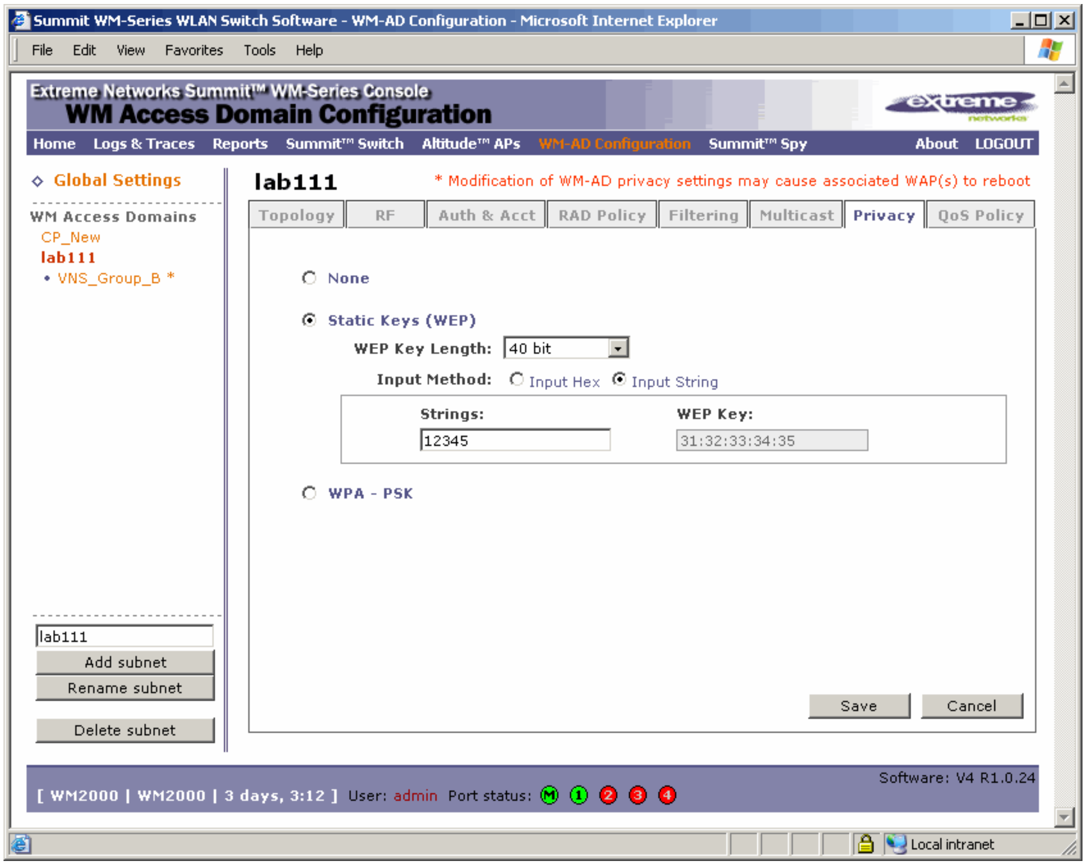
To configure privacy by static WEP for a Captive Portal WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to configure privacy by static WEP for a Captive Portal. The **Topology** tab is displayed.

3 Click the **Privacy** tab.

4 Select **Static Keys (WEP)**.



Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domains
CP_New
lab111
VNS_Group_B *
lab111
Add subnet
Rename subnet
Delete subnet
Topology RF Auth & Acct RAD Policy Filtering Multicast Privacy QoS Policy
Save
Cancel
Local intranet

lab111

* Modification of WM-AD privacy settings may cause associated WAP(s) to reboot

○ None

● Static Keys (WEP)

WEP Key Length: 40 bit

Input Method: ○ Input Hex ● Input String

Strings: 12345

WEP Key: 31:32:33:34:35

○ WPA - PSK

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

5 From the **WEP Key Length** drop-down list, select the WEP encryption key length:

- 40-bit
- 104-bit
- 128-bit

6 Select one of the following input methods:

- **Input Hex** – If you select **Input Hex**, type the WEP key input in the **WEP Key** box. The key is generated automatically, based on the input.
- **Input String** – If you select **Input String**, type the secret WEP key string used for encrypting and decrypting in the **WEP Key String** box. The WEP Key box is automatically filled by the corresponding Hex code.

7 To save your changes, click **Save**.

To configure privacy by WPA-PSK for a Captive Portal WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to configure privacy by WPA-PSK for a Captive Portal. The **Topology** tab is displayed.

3 Click the **Privacy** tab.

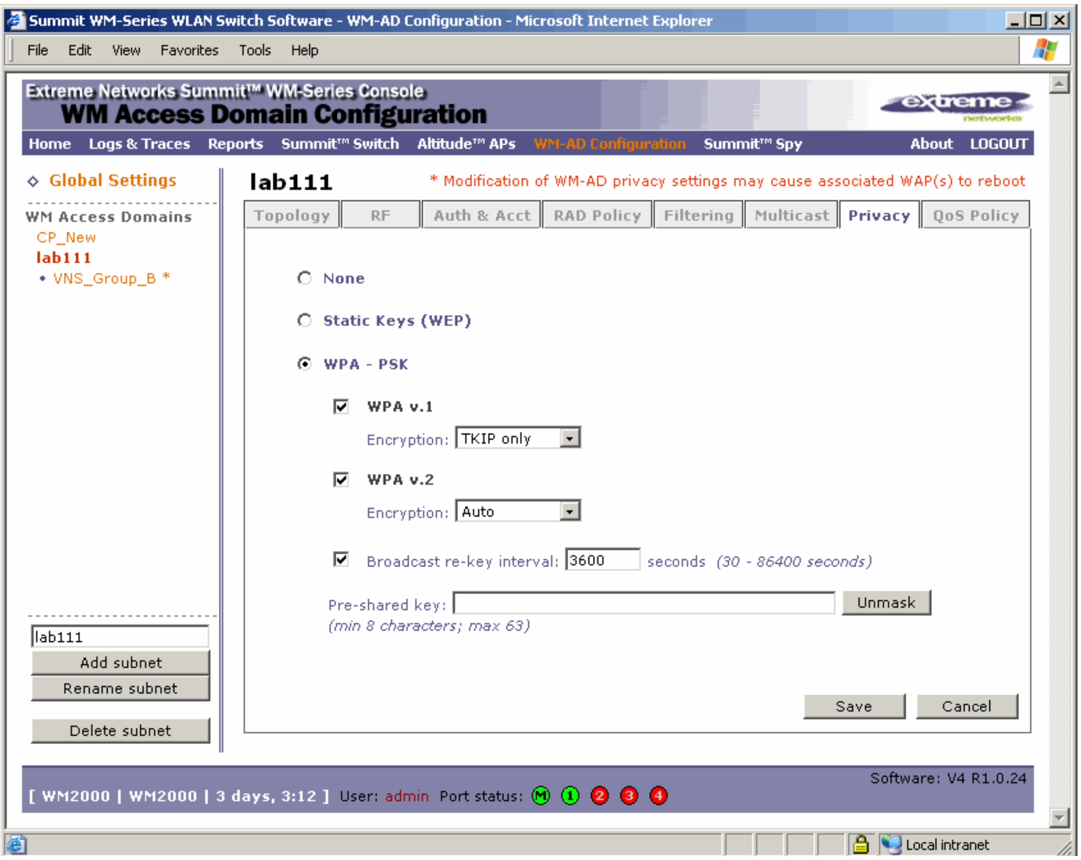
4 Select **WPA-PSK**.

5 To enable WPA v1 encryption, select **WPA v.1**.

6 If WPA v.1 is enabled, select one of the following encryption types from the **Encryption** drop-down list:

- **Auto** – The AP will advertise both TKIP and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for WPAv1. CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). Auto is the default.
- **TKIP only** – The AP will advertise TKIP as an available encryption protocol for WPAv1. It will not advertise CCMP.

7 To enable WPA v2-type encryption, select **WPA v.2**.



lab111 * Modification of WM-AD privacy settings may cause associated WAP(s) to reboot

○ None

○ Static Keys (WEP)

● WPA - PSK

☑ WPA v.1

Encryption: TKIP only

☑ WPA v.2

Encryption: Auto

☑ Broadcast re-key interval: 3600 seconds (30 - 86400 seconds)

Pre-shared key:
(min 8 characters; max 63)

lab111

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

8 To enable re-keying after a time interval, select **Broadcast re-key interval**.

If this checkbox is not selected, the Broadcast encryption key is never changed and the Altitude AP will always use the same broadcast key for Broadcast/Multicast transmissions. This will reduce the level of security for wireless communications.

9 In the **Broadcast re-key interval** box, type the time interval after which the broadcast encryption key is changed automatically. The default is 3600.

10 In the **Pre-Shared Key** box, type the shared secret key to be used between the wireless device and Altitude AP. The shared secret key is used to generate the 256-bit key.

11 In order to proofread your entry before saving the configuration, click **Unmask** to display the Pre-Shared Key. To mask the key, click **Mask**.

12 To save your changes, click **Save**.

Privacy for a WM-AD for AAA

For a WM-AD with authentication by 802.1x (AAA), there are four Privacy options:

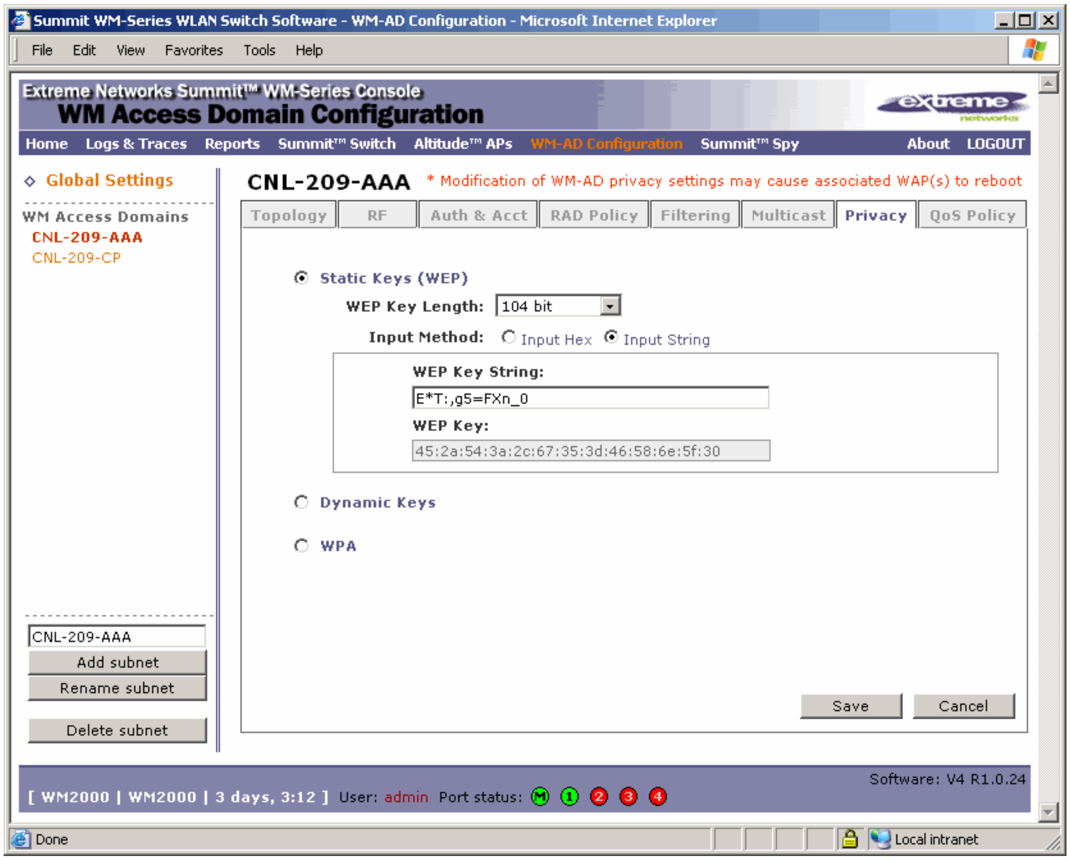
- Static keys (WEP)
- Dynamic keys
- Wi-Fi Protected Access (WPA) version 1, with encryption by Temporal Key Integrity Protocol (TKIP)
- Wi-Fi Protected Access (WPA) version 2, with encryption by Advanced Encryption Standard with Counter-Mode/CBC-MAC Protocol (AES-CCMP)

To set up static WEP privacy for an AAA WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the AAA WM-AD you want to configure privacy by WPA-PSK for a Captive Portal. The **Topology** tab is displayed.

3 Click the **Privacy** tab.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domains
CNL-209-AAA
CNL-209-CP
Topology RF Auth & Acct RAD Policy Filtering Multicast Privacy QoS Policy
Add subnet
Rename subnet
Delete subnet
Save
Cancel
Done
Local intranet

CNL-209-AAA * Modification of WM-AD privacy settings may cause associated WAP(s) to reboot

● Static Keys (WEP)

WEP Key Length: 104 bit

Input Method: ○ Input Hex ● Input String

WEP Key String: E*T:,g5=FXn_0

WEP Key: 45:2a:54:3a:2c:67:35:3d:46:58:6e:5f:30

○ Dynamic Keys

○ WPA

CNL-209-AAA

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

4 Select **Static Keys (WEP)**.

5 From the **WEP Key Length** drop-down list, select the WEP encryption key length:

- 40-bit
- 104-bit
- 128-bit

6 Select one of the following input methods:

- **Input Hex** – If you select **Input Hex**, type the WEP key input in the **WEP Key** box. The key is generated automatically, based on the input.
- **Input String** – If you select **Input String**, type the secret WEP key string used for encrypting and decrypting in the **WEP Key String** box. The WEP Key box is automatically filled by the corresponding Hex code.

7 To save your changes, click **Save**.

Dynamic WEP privacy for an AAA WM-AD

The dynamic key WEP mechanism changes the key for each user and each session.

To set up dynamic WEP privacy for a selected AAA WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane **WM Access Domains** list, click the AAA WM-AD you want to set up dynamic WEP privacy for. The **Topology** tab is displayed.

3 Click the **Privacy** tab.

4 Select **Dynamic Keys**.

5 To save your changes, click **Save**.

Wi-Fi Protected Access (WPA v1 and WPA v2) Privacy for an AAA WM-AD

The WM-AD Privacy feature supports Wi-Fi Protected Access (WPA v1 and WPA v2), a security solution that adds authentication to enhanced WEP encryption and key management.

The authentication portion of WPA for AAA is in Enterprise Mode:

- Specifies 802.1x with Extensible Authentication Protocol (EAP)
- Requires a RADIUS or other authentication server
- Uses RADIUS protocols for authentication and key distribution
- Centralizes management of user credentials

The encryption portion of WPA v1 is Temporal Key Integrity Protocol (TKIP). TKIP includes:

- A per-packet key mixing function that shares a starting key between devices, and then changes their encryption key for every packet (unicast key) or after the specified re-key time interval (broadcast key) expires
- An extended WEP key length of 256-bits
- An enhanced Initialization Vector (IV) of 48 bits, instead of 24 bits, making it more difficult to compromise

- A Message Integrity Check or Code (MIC), an additional 8-byte code that is inserted before the standard WEP 4-byte Integrity Check Value (ICV). These integrity codes are used to calculate and compare, between sender and receiver, the value of all bits in a message, which ensures that the message has not been tampered with.

The encryption portion of WPA v2 is Advanced Encryption Standard (AES). AES includes:

- A 128 bit key length, for the WPA2/802.11i implementation of AES
- Four stages that make up one round. Each round is iterated 10 times.
- A per-packet key mixing function that shares a starting key between devices, and then changes their encryption key for every packet or after the specified re-key time interval expires.
- The Counter-Mode/CBC-MAC Protocol (CCMP), a new mode of operation for a block cipher that enables a single key to be used for both encryption and authentication. The two underlying modes employed in CCM include:
  - Counter mode (CTR) that achieves data encryption
  - Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity

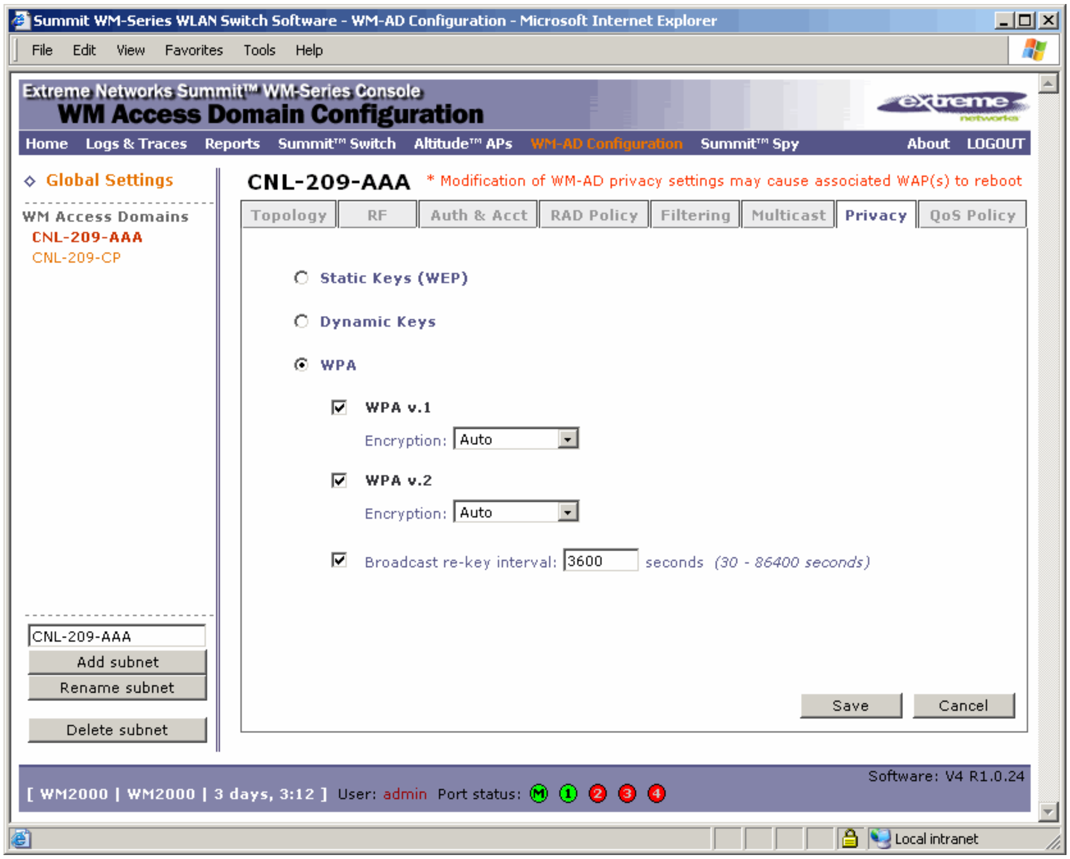
The following is an overview of the WPA authentication and encryption process:

- **Step one** – The wireless device client associates with Altitude AP.
- **Step two** – Altitude AP blocks the client's network access while the authentication process is carried out (the Summit WM series switch sends the authentication request to the RADIUS authentication server).
- **Step three** – The wireless client provides credentials that are forwarded by the Summit WM series switch to the authentication server.
- **Step four** – If the wireless device client is not authenticated, the wireless client stays blocked from network access.
- **Step five** – If the wireless device client is authenticated, the Summit WM series switch distributes encryption keys to the Altitude AP and the wireless client.
- **Step six** – The wireless device client gains network access via the Altitude AP, sending and receiving encrypted data. The traffic is controlled with permissions and policy applied by the Summit WM series switch.

To set up Wi-Fi Protected Access privacy (WPA) for an AAA WM-AD:

1. From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.
2. In the left pane **WM Access Domains** list, click the AAA WM-AD you want to configure privacy by WPA-PSK for a Captive Portal. The **Topology** tab is displayed.
3. Click the **Privacy** tab.

4 Select **WPA**.



Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domains
CNL-209-AAA
CNL-209-CP
Topology RF Auth & Acct RAD Policy Filtering Multicast Privacy QoS Policy
Add subnet
Rename subnet
Delete subnet
Save
Cancel
Local intranet

CNL-209-AAA * Modification of WM-AD privacy settings may cause associated WAP(s) to reboot

○ Static Keys (WEP)

○ Dynamic Keys

● WPA

☑ WPA v.1

Encryption: Auto

☑ WPA v.2

Encryption: Auto

☑ Broadcast re-key interval: 3600 seconds (30 - 86400 seconds)

CNL-209-AAA

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

Software: V4 R1.0.24

5 To enable WPA v1 encryption, select **WPA v.1**.

6 From the **Encryption** drop-down list, select one of the following encryption types:

- **Auto** – The AP will advertise both TKIP and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for WPAv1. CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). Auto is the default.
- **TKIP only** – The AP will advertise TKIP as an available encryption protocol for WPAv1. It will not advertise CCMP.

7 To enable re-keying after a time interval, select **Broadcast re-key interval**.

If this checkbox is not selected, the Broadcast encryption key is never changed and the Altitude AP will always use the same broadcast key for Broadcast/Multicast transmissions. This will reduce the level of security for wireless communications.

8 In the **Broadcast re-key interval** box, type the time interval after which the broadcast encryption key is changed automatically. The default is 3600.

9 To save your changes, click **Save**.

Defining a WM-AD with no authentication

You can set up a WM-AD that will bypass all authentication mechanisms and run Summit WM series switch, access points, and WLAN switch software with no authentication of a wireless device user.

A WM-AD with no authentication can still control network access using filtering rules. For more information on how to set up filtering rules that allow access only to specified IP addresses and ports, see "Defining non-authenticated filters" on page 126.

To define a WM-AD with no authentication:

1. From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.
2. In the left pane **WM Access Domains** list, click the WM-AD you want to configure with no authentication. The **Topology** tab is displayed.
3. From the **Assignment by** drop-down list, select **SSID**.
4. Configure the topology for this WM-AD, then click **Save**. For more information, see "Configuring topology for a WM-AD for Captive Portal" on page 98. You must save your changes before moving to the next tab.
5. Click the **Auth & Acct** tab.
6. Click **Configure Captive Portal Settings**. The **Captive Portal Configurations** subscreen is displayed.
7. Select **No Captive Portal Support**. You must save your changes before moving to the next tab.
8. Click the **Filtering** tab.
9. Define a default filter that will control specific network access for any wireless device users on this WM-AD. For more information, see "Configuring filtering rules for a WM-AD" on page 123.

   These rules should be very restrictive and the final rule should be a Deny All rule. The non-authenticated filter for a WM-AD with no authentication will not have a Captive Portal page for login.
10. To save your changes, click **Save**.

Defining priority level and service class for WM-AD traffic

Voice over Internet Protocol (VoIP) using 802.11 wireless local area networks are enabling the integration of internet telephony technology on wireless networks. Various issues including Quality-of-Service (QoS), call control, network capacity, and network architecture are factors in VoIP over 802.11 WLANs.

Wireless voice data requires a constant transmission rate and must be delivered within a time limit. This type of data is called isochronous data. This requirement for isochronous data is in contradiction to the concepts in the 802.11 standard that allow for data packets to wait their turn, in order to avoid data collisions. Regular traffic on a wireless network is an asynchronous process in which data streams are broken up by random intervals.

To reconcile the needs of isochronous data, mechanisms are added to the network that give voice data traffic or another traffic type priority over all other traffic, and allow for continuous transmission of data.

In order to provide better network traffic flow, the Summit WM series switch, access points, and WLAN switch software provides advanced Quality of Service (QoS) management. These management techniques include:

- **WMM (Wi-Fi Multimedia)** – Enabled globally on the Altitude AP, the standard provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS.
- **IP ToS (Type of Service) or DSCP (Diffserv Codepoint)** – The ToS/DSCP field in the IP header of a frame is used to indicate the priority and Quality of Service for each frame. The IP TOS and/or DSCP is maintained within CTP (CAPWAP Tunneling Protocol) by copying the user IP QoS information to the CTP header—this is referred to as Adaptive QoS.

Defining the service class for the WM-AD

Service class is determined by the combination of the following operations:

- The class of treatment given to a packet. For example, queuing or per hop behavior (PHB).
- The packet marking of the output packets (user traffic and/or transport).

Table 12: Service classes

Service class name (number)	Priority level
Network Control (7)	7 (highest priority)
Premium (Voice) (6)	6
Platinum (video) (5)	5
Gold (4)	4
Silver (3)	3
Bronze (2)	2
Best Effort (1)	1
Background (0)	0 (lowest priority)

The service class is equivalent to the 802.1D UP (user priority) with the exception that its scale is linear:

Table 13: Relationship between service class and 802.1D UP.

SC name	SC Value	802.1d UP	AC	Queue
Network Control	7	7	VO	VO or TVO
Premium (voice)	6	6	VO	VO or TVO
Platinum (video)	5	5	VI	VI
Gold	4	4	VI	VI
Silver	3	3	BE	BE
Bronze	2	0	BE	BE
Best Effort	1	2	BK	BK
Background	0	1	BK	BK

Configuring the priority override

Priority override allows you to define the desired priority level. Priority override can be used with any combination, as shown in Table 14. You can user is allowed to configure the service class (L2 override) and the DSCP values (L3 override values).

When **Priority Override** is enabled, the configured service class overrides the queue selection in the downlink direction, the 802.1P UP for the VLAN tagged Ethernet packets, and the UP for the wireless QoS packets (WMM or 802.11e) according to the mapping in Table 13. If **Priority Override** is enabled and the WM-AD is not locally bridged, the configured DSCP value is used to tag the IP header of the encapsulated packets. The AP does not override the DSCP in the IP header of the user packet.

Working with Quality of Service (QoS)

QoS policy is configured for each WM-AD and applies to routed, bridged at AP, and bridged at controller WM-ADs.

Each WM-AD has a configurable policy for the QoS characteristics of the WM-AD. For every user associated with the WM-AD there will be a different behavior on the wireless traffic.

NOTE

Active QoS is only applied on the wireless/802.11 domain, not on the wired domain.

QoS modes

You can enable the following Qos modes for a WM-AD:

- **Legacy** – If enabled, the AP will classify and prioritize the downlink traffic for all clients according to the same rules used for the WMM and 802.11e.
- **WMM** – If enabled, the AP will accept WMM client associations, and will classify and prioritize the downlink traffic for all WMM clients. WMM clients will also classify and prioritize the uplink traffic.
- **802.11e** – If enabled, the AP will accept WMM client associations, and will classify and prioritize the downlink traffic for all 802.11e clients. The 802.11e clients will also classify and prioritize the uplink traffic.
- **Turbo Voice** – If any of the above QoS modes are enabled, the Turbo Voice mode is available. If enabled, all the downlink traffic that is classified to the Voice (VO) AC and belongs to that WM-AD is transmitted by the AP via a queue called Turbo Voice (TVO) instead of the normal Voice (VO) queue. The TVO queue is tailored in terms of contention parameters and number of retries to maximize voice quality and voice capacity.

All combinations of the three modes are valid. The following table summarizes all possible combinations:

Table 14: QoS mode combinations

Configuration	**Legacy mode**	x		x		x		x
	WMM mode		x	x			x	x
	802.11e mode				x	x	x	x
Traffic that is classified and prioritized	**To legacy client**	x		x		x		x
	From legacy client							
	To WMM client	x	x	x		x	x	x
	From WMM client		x	x			x	x
	To 802.11e client	x		x	x	x	x	x
	From 802.11e client				x	x	x	x

The APs are capable of supporting 5 queues. The queues are implemented per radio. For example, 5 queues per radio. The queues are:

Table 15: Queues

Queue Name	Purpose
AC_VO	Voice
AC_VI	Video
AC_BK	Background
AC_BE	Best Effort
AC_TVO	Turbo Voice

The Summit WM series switch supports the definition of 8 levels of user priority (UP). These priority levels are mapped at the AP to the best appropriate access class. Of the 8 levels of user priority, 6 are considered low priority levels and 2 are considered high priority levels.

WMM clients have the same 5 AC queues. WMM clients will classify the traffic and use these queues when they are associated with a WMM-enabled AP. WMM clients will behave like non-WMM clients—map all traffic to the Best Effort (BE) queue—when not associated with WMM-enabled AP.

The prioritization of the traffic on the downstream (for example, from wired to wireless) and on the upstream (for example, from wireless to wired) is dictated by the configuration of the WM-AD and the QoS tagging within the packets, as set by the wireless devices and the host devices on the wired network.

Both Layer 3 tagging (DSCP) and Layer 2 (802.1d) tagging are supported, and the mapping is conformant with the WMM specification. If both L2 and L3 priority tags are available, then both are taken into account and the chosen AC is the highest resulting from L2 and L3. If only one of the priority tags is present, it is used to select the queue. If none is present, the default queue AC_BE is chosen.

NOTE

If the wireless packets to be transmitted must include the L2 priority (send to a WMM client from a WMM-enabled AP), the outbound L2 priority is copied from the inbound L2 priority if available, or it is inferred from the L3 priority using the above table if the L2 inbound priority is missing.

Table 16: Traffic prioritization

WM-AD type	Packet Source	Packet type	L2	L3
Tunneled	Wired	Untagged	No	Yes
Branch	Wired	VLAN tagged	Yes	Yes
Branch	Wired	Untagged	No	Yes
Branch or Tunneled	Wireless	WMM	Yes	Yes
Branch or Tunneled	Wireless	non-WMM	No	Yes

Configuring the QoS policy on a WM-AD

The following is an overview of the steps involved in configuring the QoS on a WM-AD.

Step one – Define the QoS mode to employ on the WM-AD:

- **Legacy** – Enables DL (downlink) classification for all clients
- **WMM**:
  - Enables WMM support
  - Enables DL classification for WMM clients
  - Enables UL (uplink) classification in WMM clients
- **802.11e**:
  - Enables 802.11e support
  - Enables DL classification for 802.11e clients
  - Enables UL classification in 802.11e clients

  WMM and 802.11e are similar but, they use different signaling (same as WPA and WPA2).

Step two – Enabling Turbo Voice:

- Ensures WM-AD is optimized for voice performance and capacity
- Can be enabled or disabled on individual WM-ADs
  - If Turbo Voice is enabled, together with QoS modes **Legacy**, **WMM**, or **802.11e**, DL voice traffic is sent via Turbo Voice queue instead of voice queue. A separate turbo voice queue allows for some WM-ADs to use the Turbo Voice parameters for voice traffic, while other WM-ADs use the voice parameters for voice traffic.
  - If WMM mode is also enabled, WMM clients use Turbo Voice-like contention parameters for UL voice traffic.
  - If 802.11e mode is also enabled, 802.11e clients use Turbo Voice-like contention parameters for UL voice traffic.

Step 3 – Defining the DSCP and service class classifications:

All 64 DSCP code-points are supported. The IETF defined codes are listed by name and code. Undefined codes are listed by code. The following is the default DSCP service class classification:

DSCP	SC/UP	DSCP	SC/UP	DSCP	SC/UP
CS0/DE	2/0	AF11	2/0	AF33	4/4
CS1	0/1	AF12	2/0	AF41	5/5
CS2	1/2	AF13	2/0	AF42	5/5
CS3	3/3	AF21	3/3	AF43	5/5
CS4	4/4	AF22	3/3	EF	6/6
CS5	5/5	AF23	3/3	Others	0/1
CS6	6/6	AF31	4/4		
CS7	7/7	AF32	4/4		

Step 4 – Enable Priority override:

- Select the applicable service class and implicitly desired UP
  - Updates UP in user packet
  - Updates UP for WASSP frame (if field exists) sent by AP
- Select the desired DSCP
  - Updates DSCP for WASSP frames sent by AP
  - Does not change DSCP in user packet

Step 5 – Configure the advanced wireless QoS:

- Enable the **Unscheduled Automatic Power Save Delivery** (U-APSD) feature
- Works in conjunction with WMM and/or 802.11e, and it is automatically disabled if both WMM and 802.11e are disabled

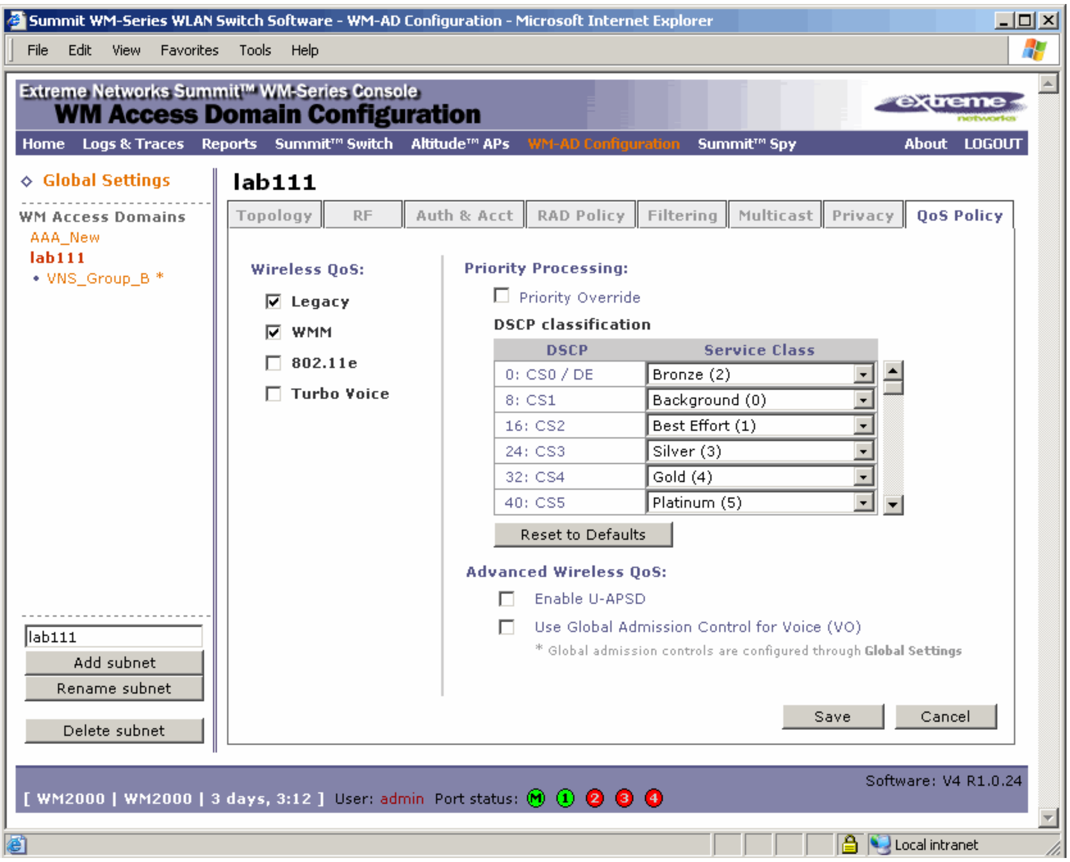
Step 5 – Configure Global Admission Control:

- Enable admission control. Admission control protects admitted traffic against new bandwidth demands.
- Available for Voice and Video.

To configure QoS Policy on a WM-AD:

1. From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.
2. In the left pane **WM Access Domains** list, click the WM-AD you want to configure for QoS.

3 Click the **QoS Policy** tab.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domains
AAA_New
lab111
• VNS_Group_B *
Topology RF Auth & Acct RAD Policy Filtering Multicast Privacy QoS Policy
Add subnet
Rename subnet
Delete subnet
Reset to Defaults
Save
Cancel
Local intranet

lab111

Wireless QoS:

☑ Legacy

☑ WMM

□ 802.11e

□ Turbo Voice

Priority Processing:

□ Priority Override

DSCP classification

DSCP	Service Class
0: CS0 / DE	Bronze (2)
8: CS1	Background (0)
16: CS2	Best Effort (1)
24: CS3	Silver (3)
32: CS4	Gold (4)
40: CS5	Platinum (5)

Advanced Wireless QoS:

□ Enable U-APSD

□ Use Global Admission Control for Voice (VO)

* Global admission controls are configured through **Global Settings**

lab111

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

4 From the **Wireless QoS** list, select the following:

- **Legacy** – Select if your WM-AD will support legacy devices that use SpectraLink Voice Protocol (SVP) for prioritizing voice traffic. If selected, the Turbo Voice option is displayed.
- **WMM** – Select to enable the AP to accept WMM client associations, and classify and prioritize the downlink traffic for all WMM clients. Note that WMM clients will also classify and prioritize the uplink traffic. WMM is part of the 802.11e standard for QoS. If selected, the **Turbo Voice** and the **Advanced Wireless QoS** options are displayed.
- **802.11e** – Select to enable the AP to accept WMM client associations, and classify and prioritize the downlink traffic for all 802.11e clients. The 802.11e clients will also classify and prioritize the uplink traffic. If selected, the **Turbo Voice** and the **Advanced Wireless QoS** options are displayed:
- **Turbo Voice** – Select to enable all downlink traffic that is classified to the Voice (VO) AC and belongs to that WM-AD to be transmitted by the AP via a queue called Turbo Voice (TVO) instead of the normal Voice (VO) queue. When **Turbo Voice** is enabled together with **WMM** or **802.11e**, the WMM and/or 802.11e clients in that WM-AD are instructed by the AP to transmit all traffic classified to VO AC with special contention parameters tailored to maximize voice performance and capacity.

5 To define the service class and DSCP marking for the WM-AD, select the **Priority Override** checkbox. For each DSCP you can select one of the eight service classes.

- **Service class** – From the drop-down list, select the appropriate priority level:
  - Network control (7) – The highest priority level.
  - Premium (Voice) (6)
  - Platinum (5)

    - Gold (4)
    - Silver (3)
    - Bronze (2)
    - Best Effort (1)
    - Background (0) – The lowest priority level
  - **DSCP marking** – From the drop-down list, select the DSCP value used to tag the IP header of the encapsulated packets.

6. If you want to assign a service class to each DSCP marking, clear the **Priority Override** checkbox and define the DSCP service class priorities in the DSCP classification table.

   When **Priority Override** is enabled, the configured service class overrides queue selection in the downlink direction, the 802.1P user priority for the VLAN tagged Ethernet packets and the user priority for the wireless QoS packets (WMM or 802.11e), according to the mapping between service class and user priority. If **Priority Override** is enabled and the WM-AD is not locally bridged, the configured DSCP value is used to tag the IP header of the encapsulated packets. The AP does not override the DSCP in the IP header of the user packet.

7. The **Advanced Wireless QoS** options are only displayed if the WMM or 802.11e checkboxes are selected:

   - **Enable U-APSD** – Select to enable the Unscheduled Automatic Power Save Delivery (U-APSD) feature. This feature can be used by mobile devices to efficiently sustain one or more real-time streams while being in power-save mode. This feature works in conjunction with WMM and/or 802.11e, and it is automatically disabled if both WMM and 802.11e are disabled.
   - **Use Global Admission Control for Voice (VO)** – Select to enable admission control for Voice. With admission control, clients are forced to request admission in order to use the high priority access categories in both downlink and uplink direction. Admission control protects admitted traffic against new bandwidth demands.
   - **Use Global Admission Control for Video (VI)** – This feature is only available If admission control is enabled for Voice. Select to enable admission control for Video. With admission control, clients are forced to request admission in order to use the high priority access categories in both downlink and uplink direction. Admission control protects admitted traffic against new bandwidth demands.

8. To save your changes, click **Save**.

Bridging traffic locally

A WM-AD must first be setup before traffic can be bridged locally. For more information, see Chapter 4, "WM Access Domain Services (WM-AD)."

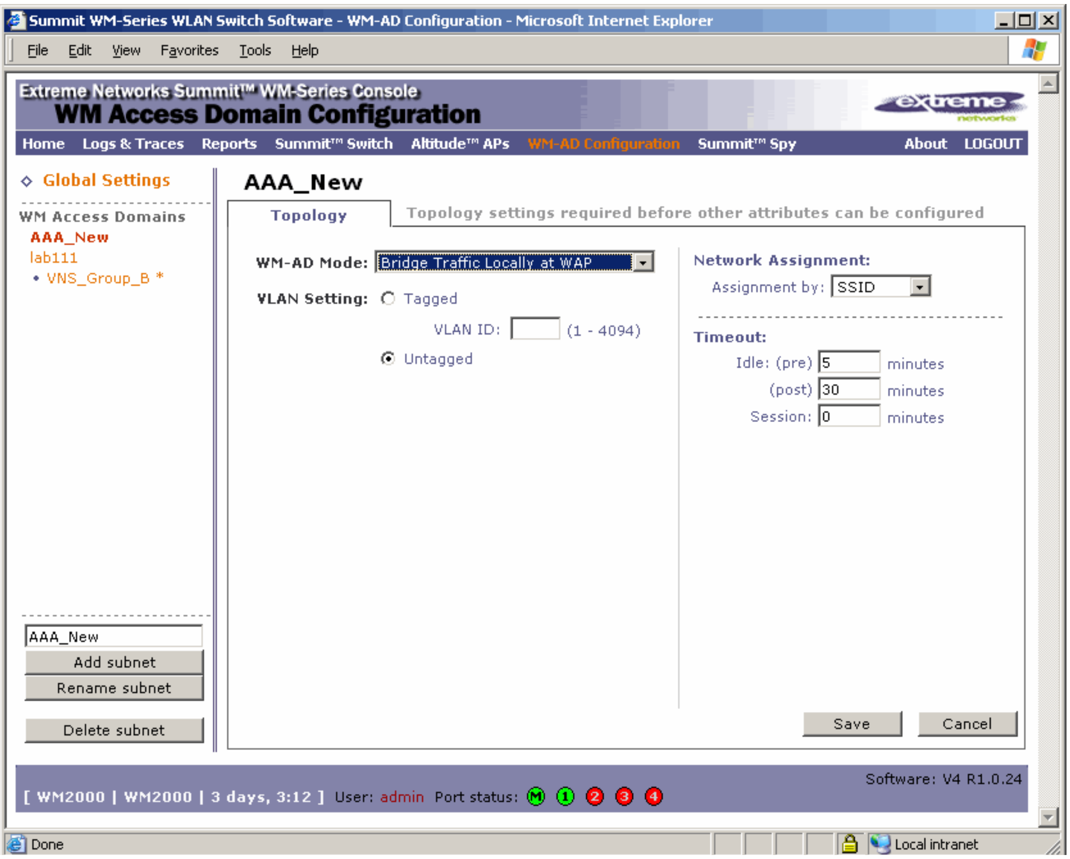
To bridge traffic locally:

1. From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.
2. In the left pane **WM Access Domains** list, click the WM-AD that you want to define topology parameters for.
3. Click the **Topology** tab.
4. In the **WM-AD Mode** drop-down list, click **Bridge Traffic Locally at AP** to enable branch office mode.

5 To define the VLAN Setting, select one of the following:

- Tagged
- Untagged

If you select **Tagged**, type the VLAN ID in the **VLAN ID** box. The default value is 1.



Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domains
AAA_New
lab111
VNS_Group_B *
Add subnet
Rename subnet
Delete subnet
Topology
Save
Cancel
Done
Local intranet

AAA_New

Topology settings required before other attributes can be configured

WM-AD Mode: Bridge Traffic Locally at WAP

VLAN Setting: ○ Tagged

VLAN ID: (1 - 4094)

● Untagged

Network Assignment:

Assignment by: SSID

Timeout:

Idle: (pre) 5 minutes

(post) 30 minutes

Session: 0 minutes

AAA_New

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

NOTE

The VLAN IDs are assigned by the branch office network administrator. The AP will operate correctly only if the VLAN ID is unique per AP.

Configuring two untagged branch WM-ADs to the same AP on different radios is permitted. This is similar to having two untagged branch WM-ADs with the same VLAN ID assigned to the same AP on different radios. In both cases, the AP will connect the two WM-ADs. That type of configuration can be viewed as a single WM-AD/ VLAN with different SSIDs on different radios.

An effective scenario of the configuration described above, in which the same subnet is used with different SSIDs on radio a and b/g, is when this configuration is defined consistently on all APs. It would allow dual band a+b/g clients to associate to one of the radios by specifying the correct SSID. This is particularly effective with Microsoft clients, which do not allow defining a preferred radio.

6 To save your changes, click **Save**.

NOTE

In previous releases, an entire AP had to be put into branch mode. In the current release, an individual WM-AD can be put into bridging mode. An AP can have bridged and non-bridged WM-ADs.

If it has more then one branch mode WM-AD, only one bridged WM-AD can be untagged per AP. The other branch mode WM-ADs need to have unique VLAN ID. You must have VLAN aware L2 switches to support this feature.

NOTE

When a WM-AD is setup for bridged mode, it cannot be switched to tunneled mode. The administrator must delete and re-add the WM-AD.

6 Availability, mobility, and controller functionality

This chapter describes the availability and mobility concepts, including:

- Availability overview
- Mobility manager
- Defining management users
- Configuring network time
- Configuring Check Point event logging
- Enabling SNMP
- Using controller utilities
- Configuring Web session timeouts

The Summit WM series switch provides additional functionality including:

- **Availability** – Maintains service availability in the event of a Summit WM series switch outage
- **Mobility** – Allows multiple Summit WM series switches on a network discover each other and exchange information about a client session. A maximum of up to 8 controllers can be linked to allow users to transparently roam across controllers in the mobility domain.

Availability overview

The Summit WM series switch, access points, and WLAN switch software system provides this feature to maintain service availability in the event of a Summit WM series switch outage.

The availability feature links two Summit WM series switches as a pair, to share information about their Altitude APs. If one controller fails, its Altitude APs are allowed to connect to the backup controller. The second Summit WM series switch provides the wireless network and a pre-assigned WM Access Domain Service (WM-AD) for the Altitude AP.

NOTE

The Summit WM series switch's mobility domain licence (MDL) limits the number of APs that are allowed to connect to the controller. During a failover event, the maximum number of failover APs a backup controller can accommodate is equal to the number of MDLs that are purchased for that system.

NOTE

Altitude APs that attempt to connect to a backup controller during a failover event are assigned to the WM-AD that is defined in the system's default AP configuration. If a system default AP configuration does not exist for the controller, the failover AP will not be assigned to any WM-AD.

Also, the default AP configuration assignment is only applicable to new APs that failover to the backup controller. Any AP that has previously failed-over and is already known to the backup system will receive the configuration already present on that system.

For more information, see "Configuring the default AP settings" on page 66.

From the viewpoint of an Altitude AP, if a Summit WM series switch or the connection to it fails, the Altitude AP begins its discovery process. The Altitude AP is directed to the appropriate backup controller of the pair. This connection may require the Altitude AP to reboot. Users on the Altitude AP must log in again and be authenticated on the second Summit WM series switch.

NOTE

The availability feature provides APs with a list of interfaces to which the AP should attempt to automatically connect to when a connection with an active controller link is lost. The provided list identifies the local active interfaces (enabled on the primary and backup controllers) for the active controller as well as the active interfaces for the backup controller. The list is sorted by top-down priority. If the active link is lost (poll failure), the AP automatically scans (pings) all addresses in its availability interface list. The AP will then connect to the highest priority interface that responds to its probe.

Availability prerequisites

Before you begin, ensure you have completed the following:

- Choose the primary and secondary Summit WM series switches.
- Verify the network accessibility for the TCP/IP connection between the two switches. The availability link is established as a TCP session on port 13907.
- Set up a DHCP server for AP subnets to support Option 78 for SLP, so that it points to the IP addresses of the physical interfaces on both Summit WM series switches.

Now set up each Summit WM series switch separately. One method is as follows:

1. In the **AP Registration** screen, set up each Summit WM series switch in Stand-alone Mode and Secure Mode (allow only approved Altitude APs to connect).
2. In the **Topology** tab, define a WM-AD on each Summit WM series switch with the same SSID. The IP addresses must be unique. For more information, "Topology for a WM-AD" on page 98. A Summit WM series switch WM200/2000 VLAN Bridged WM-AD can permit two controllers to share the same subnet (different IP addresses). This setup provides support for mobility users in a VLAN Bridged WM-AD.
3. On both Summit WM series switches, set the Registration Mode to Allow only approved so that no more Altitude APs can register unless they are approved by the administrator.
4. In the **AP Registration** screen, enable the two Summit WM series switches as an availability pair.
5. On each Summit WM series switch, in the **Access Approval** screen, check the status of the Altitude APs and approve any APs that should be connected to that controller.

   System AP defaults can be used to assign a group of WM-ADs to the foreign APs:

   - If the APs are not yet known to the system, the AP will be initially configured according to AP default settings. To ensure better transition in availability, it is recommended that the AP default settings match the desired WM-AD assignment for failover APs.
   - AP assignment to WM-ADs according to the AP default settings can be overwritten by manually modifying the AP WM-AD assignment. (For example, select and assign each WM-AD that the AP should connect to.)
   - If specific foreign APs have been assigned to a WM-AD, those specific foreign AP assignments are used.

An alternate method to setting up APs includes:

1 Add each Altitude AP manually to each Summit WM series switch.

2 From the **AP Properties** screen, click **Add Altitude AP**.

3 Define the Altitude AP and click **Add Altitude AP**.

Manually defined APs will inherit the default AP configuration settings.

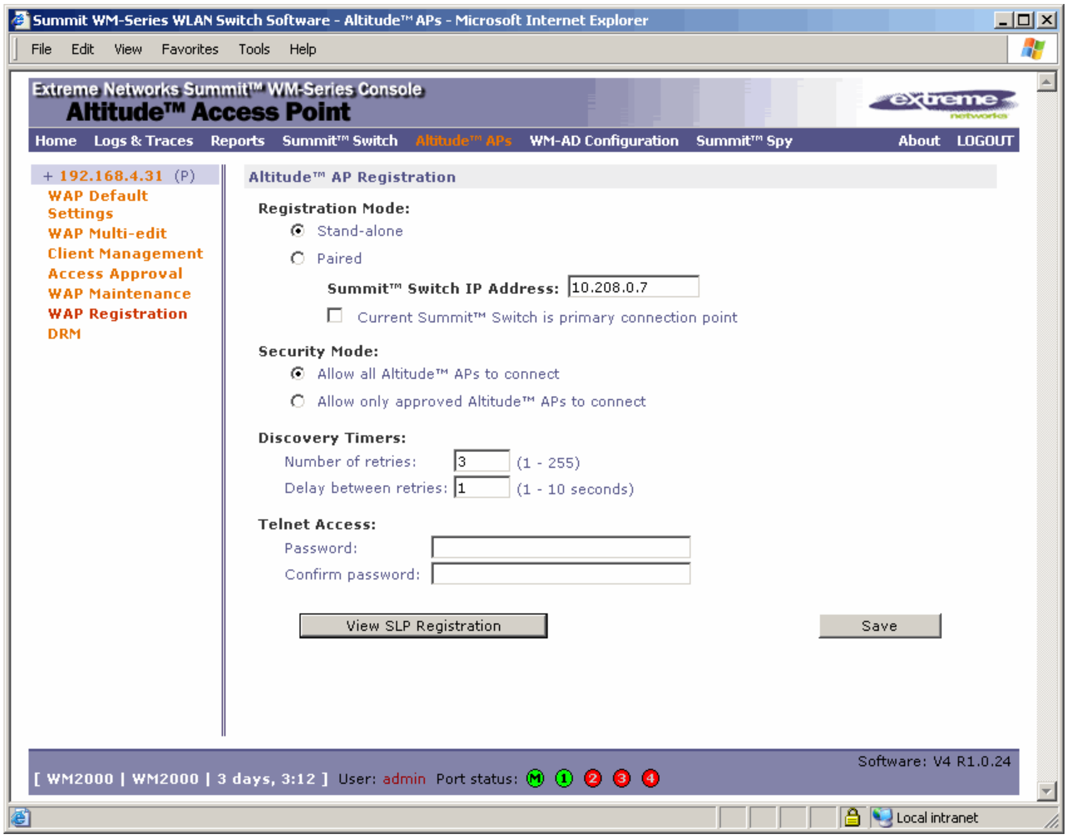
WARNING!

If two Summit WM series switches are paired and one has the Allow All option set for Altitude AP registration, all Altitude APs will register with that Summit WM series switch.

To set the primary or secondary Summit WM series switches for availability:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** screen is displayed.

2 In the left pane, click **AP Registration**. The **Altitude AP Registration** screen is displayed.


Summit WM-Series WLAN Switch Software - Altitude™ APs - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Altitude™ Access Point
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
+ 192.168.4.31 (P)
WAP Default Settings
WAP Multi-edit
Client Management
Access Approval
WAP Maintenance
WAP Registration
DRM
View SLP Registration
Save
Local intranet

Altitude™ AP Registration

Registration Mode:

◉ Stand-alone

○ Paired

Summit™ Switch IP Address: 10.208.0.7

☐ Current Summit™ Switch is primary connection point

Security Mode:

◉ Allow all Altitude™ APs to connect

○ Allow only approved Altitude™ APs to connect

Discovery Timers:

Number of retries: 3 (1 - 255)

Delay between retries: 1 (1 - 10 seconds)

Telnet Access:

Password:

Confirm password:

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

3 To enable availability, select the **Paired** option.

4 Do one of the following:

- For a primary controller, in the **Summit Switch IP Address** box, type the IP address of the physical port of the secondary Summit WM series switch. This IP address must be on a routable subnet between the two Summit WM series switches.
- For a secondary controller, in the **Summit Switch IP Address** box, type the IP address of the Management port or physical port of the primary Summit WM series switch.

5 Do one of the following:

- To set this Summit WM series switch as the primary connection point, select the **Current Summit Switch is primary connect point** checkbox.
- To set this Summit WM series switch as the secondary connection point, clear the **Current Summit Switch is primary connect point** checkbox.

If the **Current Wireless Switch is primary connect point** checkbox is selected, the specified switch waits for a request. If the **Current Wireless Switch is primary connect point** checkbox is cleared, the specified switch sends a connection request. Confirm that one switch has this checkbox selected, and the second switch has this checkbox cleared, since improper configuration of this option will result in incorrect network configuration.

6 To set the security mode for the Summit WM series switch, select one of the following options:

- **Allow all Altitude APs to connect** – If the Summit WM series switch does not recognize the serial number, it sends a default configuration to the Altitude AP. Or, if the Summit WM series switch recognizes the serial number, it sends the specific configuration (port and binding key) set for that Altitude AP.
- **Allow only approved Altitude APs to connect –** If the Summit WM series switch does not recognize the serial number, the operator is prompted to create a configuration. Or, if the Summit WM series switch recognizes the serial number, it sends the configuration for that Altitude AP.

NOTE

During the initial setup of the network, it is recommended to select the Allow all Altitude APs to connect option. This option is the most efficient way to get a large number of Altitude APs registered with the Summit WM series switch.

Once the initial setup is complete, it is recommended that the security mode is reset to the Allow only approved Altitude APs to connect option. This option ensures that no unapproved Altitude APs are allowed to connect. For more information, see "Modifying Altitude AP settings" on page 64.

7 To save your changes, click **Save**.

NOTE

When two Summit WM series switches have been paired as described above, each Summit WM series switch's registered Altitude APs will appear as foreign on the other controller in the list of available Altitude APs when configuring a WM-AD topology.

Viewing the Altitude AP availability display

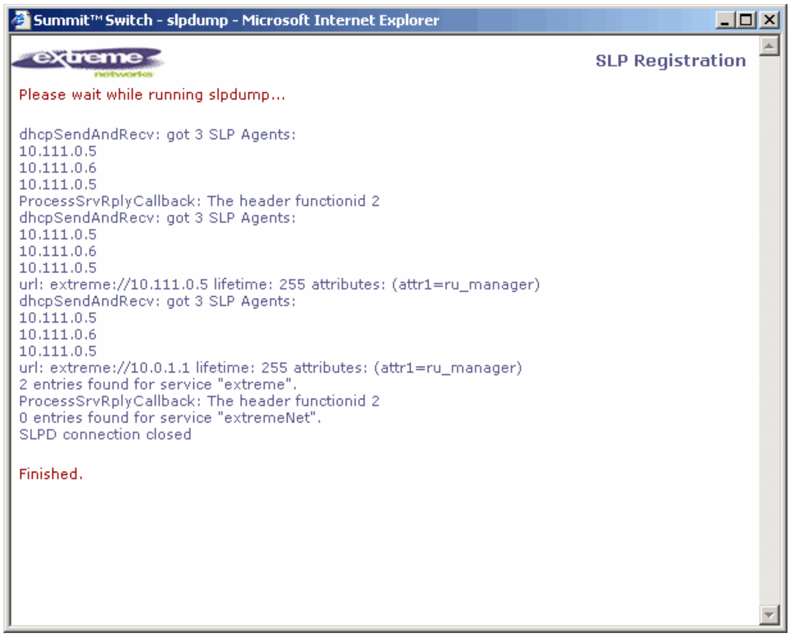
For more information, see "Viewing the Altitude AP availability display" on page 193.

Viewing SLP activity

In normal operations, the primary Summit WM series switch registers as an SLP service called ac_manager. The controller service directs the Altitude APs to the appropriate Summit WM series switch. During an outage, if the remaining Summit WM series switch is the secondary controller, It registers as the SLP service ru_manager.

To view SLP activity:

1. From the main menu, click **Altitude AP Configuration**. The **Altitude APs** screen is displayed.
2. In the left pane, click **AP Registration**. The **Altitude AP Registration** screen is displayed.
3. To confirm SLP registration, click the **View SLP Registration** button. A pop-up screen displays the results of the diagnostic slpdump tool, to confirm SLP registration.



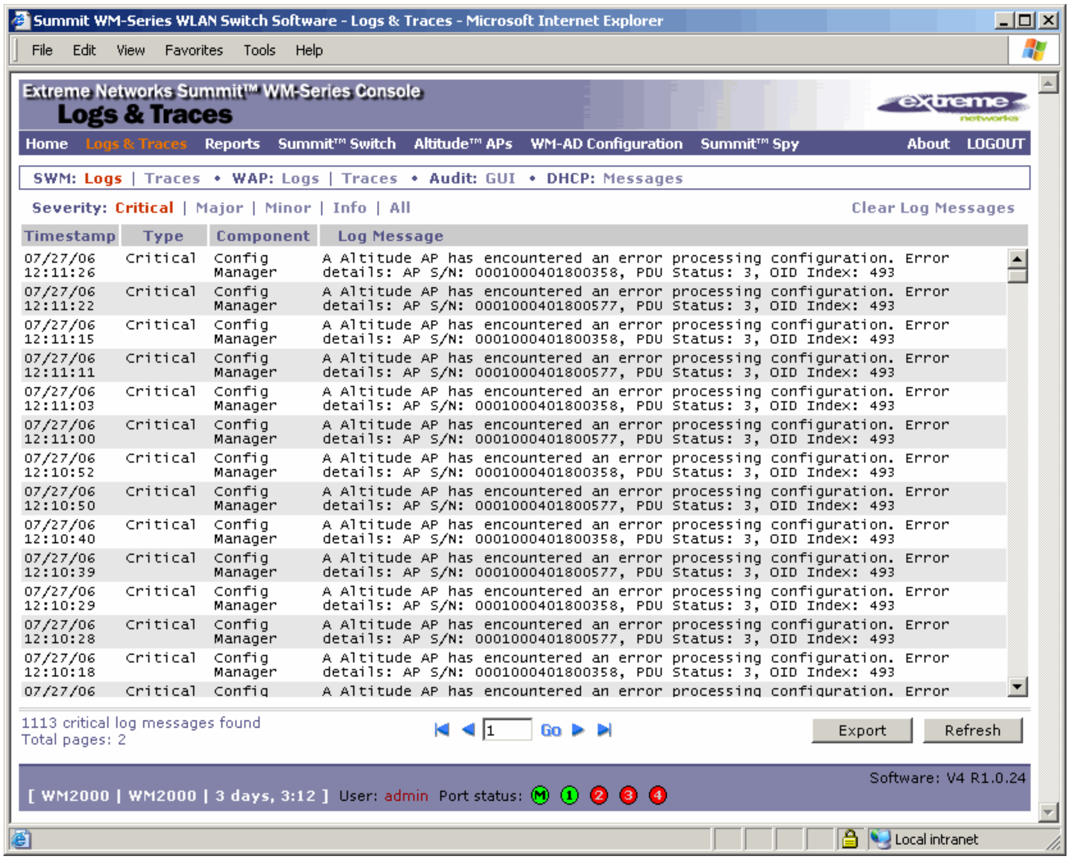
```
Please wait while running slpdump...

dhcpSendAndRecv: got 3 SLP Agents:
10.111.0.5
10.111.0.6
10.111.0.5
ProcessSrvRplyCallback: The header functionid 2
dhcpSendAndRecv: got 3 SLP Agents:
10.111.0.5
10.111.0.6
10.111.0.5
url: extreme://10.111.0.5 lifetime: 255 attributes: (attr1=ru_manager)
dhcpSendAndRecv: got 3 SLP Agents:
10.111.0.5
10.111.0.6
10.111.0.5
url: extreme://10.0.1.1 lifetime: 255 attributes: (attr1=ru_manager)
2 entries found for service "extreme".
ProcessSrvRplyCallback: The header functionid 2
0 entries found for service "extremeNet".
SLPD connection closed

Finished.
```

Events and actions during a failover

If one of the Summit WM series switches in a pair fails, the connection between the two Summit WM series switches is lost. This triggers a failover mode condition, and a critical message is displayed in the information log of the remaining Summit WM series switch.


Summit WM-Series WLAN Switch Software - Logs & Traces - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Logs & Traces
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
SWM: Logs | Traces • WAP: Logs | Traces • Audit: GUI • DHCP: Messages
Severity: Critical | Major | Minor | Info | All
Clear Log Messages
Go
Export
Refresh
Local intranet

Timestamp	Type	Component	Log Message
07/27/06 12:11:26	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:11:22	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:11:15	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:11:11	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:11:03	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:11:00	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:10:52	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:10:50	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:10:40	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:10:39	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:10:29	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:10:28	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:10:18	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06	Critical	Config	A Altitude AP has encountered an error processing configuration. Error

1113 critical log messages found
Total pages: 2

1

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: Ⓜ ① ② ③ ④

After the Altitude AP on the failed Summit WM series switch loses its connection, it will try to connect to all enabled interfaces on both controllers without rebooting. If the Altitude AP is unsuccessful, it will begin the discovery process. If the Altitude AP is not successful in connecting to the Summit WM series switch after five minutes of attempting, the Altitude AP will reboot.

If the AP is assigned to different WM-ADs on the two controllers, it will reboot. Because of the pairing of the two Summit WM series switches, the Altitude AP will then register with the other Summit WM series switch.

All user sessions using the AP that fails over will terminate unless the **Maintain client sessions in event of poll failure** option is enabled on the **AP Properties** tab or **AP Default Settings** screen.

NOTE

An Altitude AP connects first to a Summit WM series switch registered as ac_manager and, if not found, then seeks an ru_manager. If the primary Summit WM series switch fails, the secondary one registers as ru_manager. This enables the secondary Summit WM series switch to be found by Altitude APs after they reboot.

When the Altitude APs connect to the second Summit WM series switch, they will be assigned to the WM-AD that is defined in the system's default AP configuration. The wireless device users will log in again and be authenticated on the second Summit WM series switch.

When the failed Summit WM series switch recovers, each Summit WM series switch in the pair goes back to normal mode. They exchange information that includes the latest lists of registered Altitude APs. The administrator must release the Altitude APs manually on the second Summit WM series switch, so that they may re-register with their home Summit WM series switch. Foreign APs can now all be released at once by using the **Foreign** button on the Access Approval screen to select all foreign APs, and then clicking **Released**.

To support the availability feature during a failover event, administrators need to do the following:

1. Monitor the critical messages for the failover mode message, in the information log of the remaining Summit WM series switch (in the **Reports and Displays** section of the Summit WM series switch).
2. After recovery, on the Summit WM series switch that did not fail, select the foreign Altitude APs and click on the **Release** button on the **Access Approval** screen.

Mobility manager

The Summit WM series switch, access points, and WLAN switch software system allows multiple Summit WM series switches (up to 8) on a network discover each other and exchange information about a client session. This technique enables a wireless device user to roam seamlessly between different Altitude APs on different Summit WM series switches.

The solution introduces the concept of a mobility manager, where one Summit WM series switch on the network is designated as the mobility manager and all others are designated as mobility agents.

The wireless device keeps the IP address, WM-AD assignment, and filtering rules it received from its home Summit WM series switch—the Summit WM series switch that it first connected to. The WM-AD on each Summit WM series switch must have the same SSID and RF privacy parameter settings.

NOTE

For the mobility manager you have two options:

> Rely on SLP with DHCP Option 78.

> Define at the agent the IP address of the mobility manager. By explicitly defining the IP address, the agent and the mobility manager are able to find each other directly without using the SLP discovery mechanisms. Direct IP definition is recommended in order to provide tighter control of the registration steps for multi-domain installations.

The Summit WM series switch designated as the mobility manager:

- The mobility manager is explicitly identified as the manager for a specific mobility domain. Agents will connect to this manager to establish a mobility domain.
- Defines at the agent the IP address of the mobility manager, which allows for the bypass of SLP. Agents directly find and attempt to register with the mobility manager.
- Uses SLP, if this method is preferred, to register itself with the SLP Directory Agent as ExtremeNet

- Defines the registration behavior for a multi-controller mobility domain set:
  - **Open mode –** A new agent is automatically able to register itself with the mobility manager and immediately becomes part of the mobility domain
  - **Secure mode** – The mobility manager does not allow a new agent to automatically register. Instead, the connection with the new agent is placed in pending state until the administrator approves the new device.
- Listens for connection attempts from mobility agents
- Establishes connection and sends a message to the mobility agent specifying the Heartbeat interval, and the mobility manager's IP address if it receives a connection attempt from the agent
- Sends regular Heartbeat messages containing wireless device session changes and agent changes to the mobility agents and waits for a returned update message

The Summit WM series switch designated as a mobility agent:

- Uses SLP or a statically configured IP address to locate the mobility manager
- Defines at the agent the IP address of the mobility manager, which allows for the bypass of SLP. Agents directly find and attempt to register with the mobility manager.
- Attempts to establish a TCP/IP connection with the mobility manager
- Updates its tables, and sets up data tunnels to and between all Summit WM series switches it has been informed of when it receives the connection-established message
- Uses the information from every Heartbeat message received to update its own tables and updates the mobility manager with information on the wireless device users and data tunnels it is managing

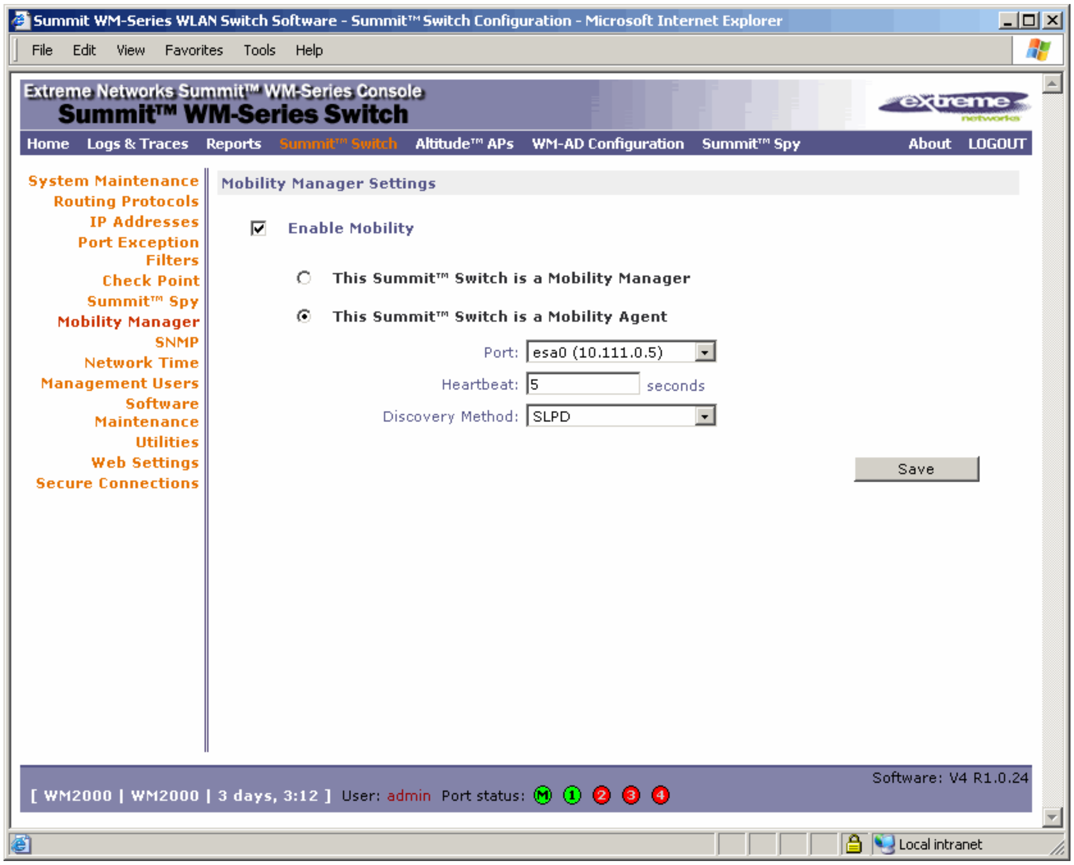
If a controller configured as the mobility manager is lost, the following occurs:

- Agent to agent connections will remain active.
- Mobility agents will continue to operate based on the mobility information last coordinated before the manager link was lost. The mobility location list remains relatively unaffected by the controller failure. Only entries associated with the failed controller are cleared from the registration list, and users that have roamed from the manager controller to other agents are terminated and required to re-register as local users with the agent where they are currently located.
- Participant controllers are reset to nodal operation
- Any user sessions that roamed away from their home AP are terminated and must reconnect
- Users need to reconnect to network, re-authenticate, and obtain new IP address
- The data link between active controllers remains active after the loss of a mobility manager
- Mobility agents continue to use the last set of mobility location list to service known users
- Existing users:
  - Existing users remain in mobility scenario, and if the users are known to mobility domain, they continue to be able to roam between connected controllers
- New users:
  - New users become local at attaching controller
  - Roaming to another controller resets session

To designate a mobility manager:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 In the left pane, click **Mobility Manager**. The **Mobility Manager Settings** screen is displayed.



Mobility Manager Settings

☑ Enable Mobility

○ This Summit™ Switch is a Mobility Manager

● This Summit™ Switch is a Mobility Agent

Port: esa0 (10.111.0.5)

Heartbeat: 5 seconds

Discovery Method: SLPD

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

3 To enable mobility for this controller, select the **Enable Mobility** checkbox. The controller mobility options appear.

4 Select the **This Summit Switch is a Mobility Manager** option. The mobility manager options appear.

5 In the **Port** drop-down list, select the interface on the Summit WM series switch to be used for the mobility manager process. Ensure that the selected interface is routable on the network.

6 In the **Heartbeat** box, type the time interval (in seconds) at which the mobility manager sends a Heartbeat message to a mobility agent. The default is **5** seconds.

7 In the **SLP Registration** drop-down list, select whether to enable or disable SLP registration.

8 In the **Permission** list, select the agent IP addresses you want to approve that are in pending state, by selecting the agent and clicking **Approve**. New agents are only added to the domain if they are approved.

You can also add or delete controllers that you want to be part of the mobility domain. To add a controller, type the agent IP address in the box, and then click **Add**. To delete a controller, select the controller in the list, and then click **Delete**.

9 Select the Security Mode option:

- **Allow all mobility agents to connect** – All mobility agents can connect to the mobility manager.
- **Allow only approved mobility agents to connect** – Only approved mobility agents can connect to the mobility manager.

10 To save your changes, click **Save**.

NOTE

If you set up one Summit WM series switch on the network as a mobility manager, all other Summit WM series switches must be set up as mobility agents.

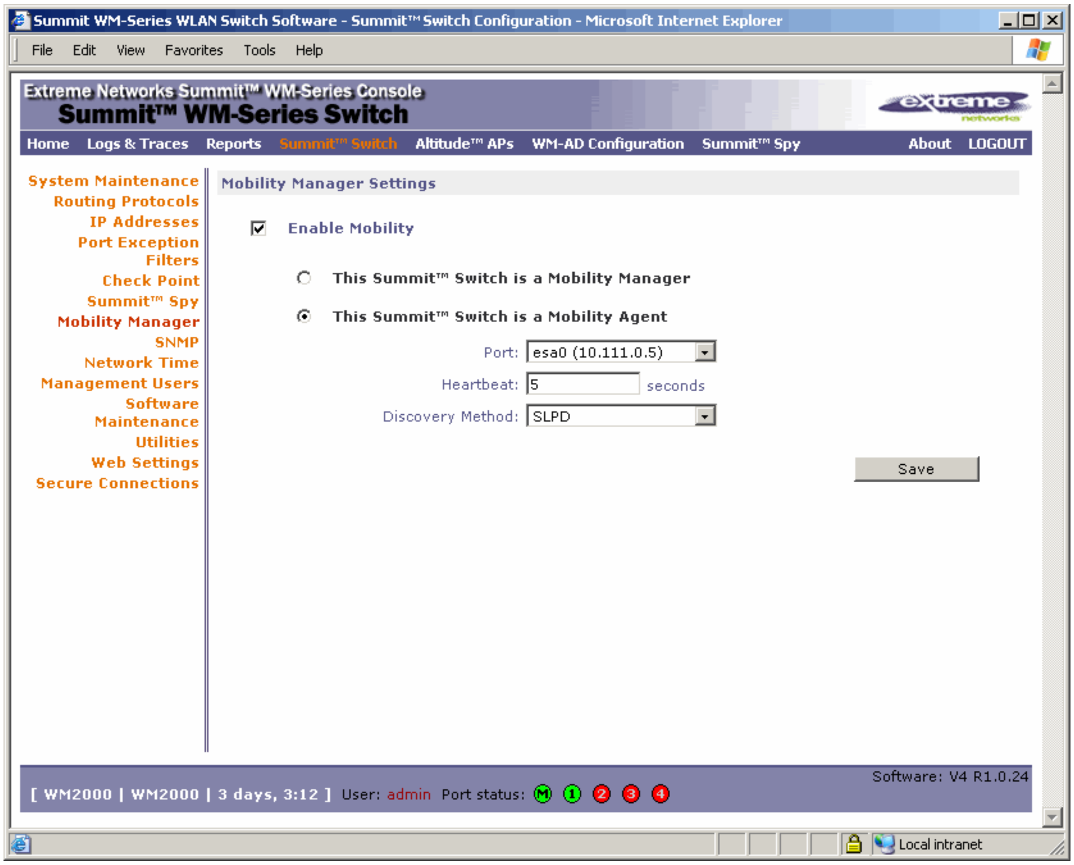
To designate a mobility agent:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 In the left pane, click **Mobility Manager**. The **Mobility Manager Settings** screen is displayed.

3 To enable mobility for this controller, select the **Enable Mobility** checkbox. The controller mobility options appear,

4 Select the **This Summit Switch is a Mobility Agent** option. The mobility agent options appear.


Summit WM-Series WLAN Switch Software - Summit™ Switch Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Switch
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
System Maintenance
Routing Protocols
IP Addresses
Port Exception Filters
Check Point
Summit™ Spy
Mobility Manager
SNMP
Network Time
Management Users
Software Maintenance
Utilities
Web Settings
Secure Connections
Save
Local intranet

Mobility Manager Settings

☑ Enable Mobility

○ This Summit™ Switch is a Mobility Manager

● This Summit™ Switch is a Mobility Agent

Port: esa0 (10.111.0.5)

Heartbeat: 5 seconds

Discovery Method: SLPD

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

5 In the **Port** drop-down list, select the port on the Summit WM series switch to be used for the mobility agent process. Ensure that the port selected is routable on the network.

6 In the **Heartbeat** box, type the time interval (in seconds) to wait for a connection establishment response before trying again. The default is **60** seconds.

7 From the **Discovery Method** drop-down list, select one of the following:

- **SLPD** – Service Location Protocol Daemon is a background process acting as a SLP server. It provides the functionality of the Directory Agent and Service Agent for SLP. Use SLP to support the discovery of extremeNET service to attempt to locate the area mobility manager controller.
- **Static Configuration** – Select Static Configuration if you want to enter the IP address of the mobility manager manually. Defining a static configuration for a mobility manager IP address bypasses SLP discovery.

8 In the **Mobility Manager Address** box, type the IP address for the designated mobility manager.

9 To save your changes, click **Save**.

Displays for the mobility manager

For more information, see "Viewing displays for the mobility manager" on page 196.

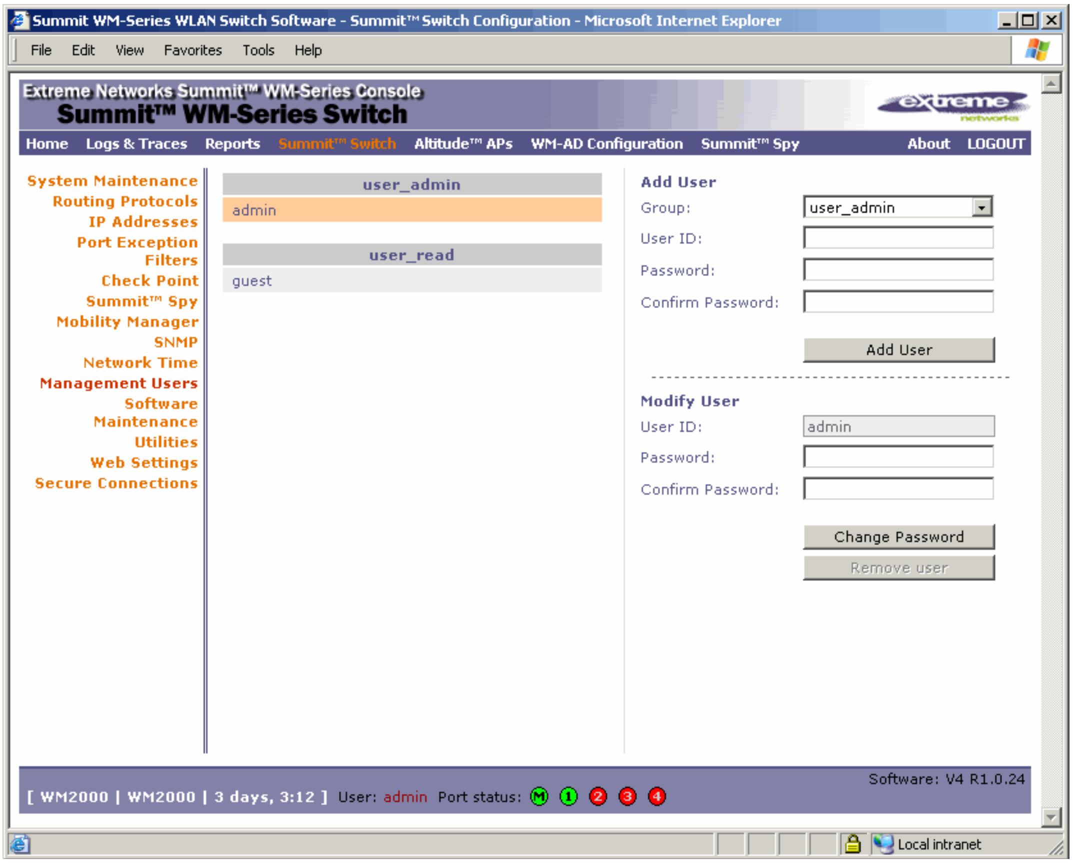
Defining management users

In this screen you define the login user names that have access to the Summit Wireless Assistant, either for Summit WM series switch, access points, and WLAN switch software administrators with read/ write privileges, or users with read only privileges. For each user added, you can also define and modify a user ID and password.

To add a Summit WM series switch management user:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 In the left pane, click the **Management Users** option. The **Management Users** screen is displayed.



user_admin: admin

user_read: guest

Group: user_admin

User ID:

Password:

Confirm Password:

User ID: admin

Password:

Confirm Password:

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

The **user_admin** list displays Admin users who have read/write privileges. The **user_read** list is for users who have read only privileges.

3 From the **Group** pull-down list, select **Admin** or **Read only**.

4 In the **User ID** box, type the user ID for the new user. A User ID can only be used once, in only one category.

5 In the **Password** box, type the password for the new user.

6 In the **Confirm Password**, retype the password. The $ character is not permitted.

7 Click on the **Add User** button. The new user is added to the appropriate user list.

To modify a Summit WM series switch management user:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 In the left pane, click the **Management Users** option. The **Management Users** screen is displayed.

3 To select a user to be modified, click it.

4 In the **Password** box, type the new password for the user.

5 In the **Confirm Password**, retype the new password.

6 To change the password, click **Change Password**.

To remove a Summit WM series switch management user:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 In the left pane, click the **Management Users** option. The **Management Users** screen is displayed.

3 To select a user to be removed, click it.

4 To remove the user, click **Remove user**. The user if removed from the list.

Configuring network time

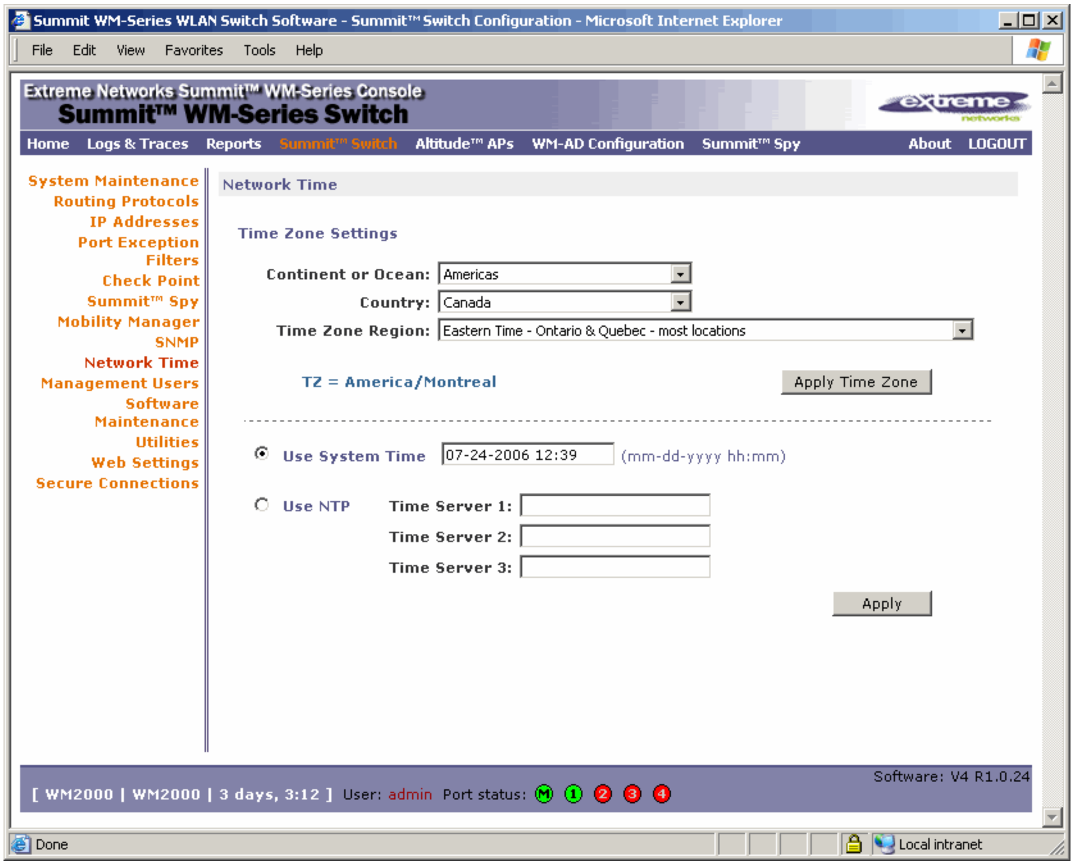
You can synchronize the elements on the network to a universal clock. This ensures accuracy in usage logs. Network time is synchronized in one of two ways:

- using system time
- using Network Time Protocol (NTP), an Internet standard protocol that synchronizes client workstation clocks.

To apply time zone settings:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 In the left pane, click **Network Time**. The **Network Time** screen is displayed.



Network Time

Time Zone Settings

Continent or Ocean: Americas

Country: Canada

Time Zone Region: Eastern Time - Ontario & Quebec - most locations

TZ = America/Montreal

● Use System Time 07-24-2006 12:39 (mm-dd-yyyy hh:mm)

○ Use NTP Time Server 1: Time Server 2: Time Server 3:

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

3 From the **Continent or Ocean** drop-down list, select the appropriate large-scale geographic grouping for the time zone.

4 From the **Country** drop-down list, select the appropriate country for the time zone. The contents of the drop-down list change based on the selection in the **Continent or Ocean** drop-down list.

5 From the **Time Zone Region** drop-down list, select the appropriate time zone region for the selected country.

6 To apply your changes, click **Apply Time Zone**.

To set system time parameters:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 In the left pane, click **Network Time**. The **Network Time** screen is displayed.

3 To use system time, select the **Use System Time** radio button.

4 Type the time setting in the **Use System TIme** box, using the mm-dd-yyyy hh:mm format.

5 To apply your changes, click **Apply.**

To set Network Time Protocol:

1. From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
2. In the left pane, click **Network Time**. The **Network Time** screen is displayed.
3. To use Network Time Protocol, select the **Use NTP** radio button.
4. In the **Use System TIme** box, type the time setting using the mm-dd-yyyy hh:mm format.
5. In the **Time Server 1** box, type the IP address or FQDN of a standard NTP Time Server. You can repeat this step for the **Time Server 2** and **Time Server 3** boxes.
6. To apply your changes, click **Apply**.

Configuring Check Point event logging

The Summit WM series switch can forward specified event messages to an ELA server using the OPSEC ELA protocol - Event Logging API (Application Program Interface). On the ELA server, the event messages are tracked and analyzed, so suspicious messages can be forwarded to a firewall application that can take corrective action.

Check Point created the OPSEC (Open Platform for Security) alliance program for security application and appliance vendors to enable an open industry-wide framework for inter operability.

When ELA is enabled on the Summit WM series switch, it forwards the specified event messages from its internal event server to the designated ELA Management Station on the enterprise network.

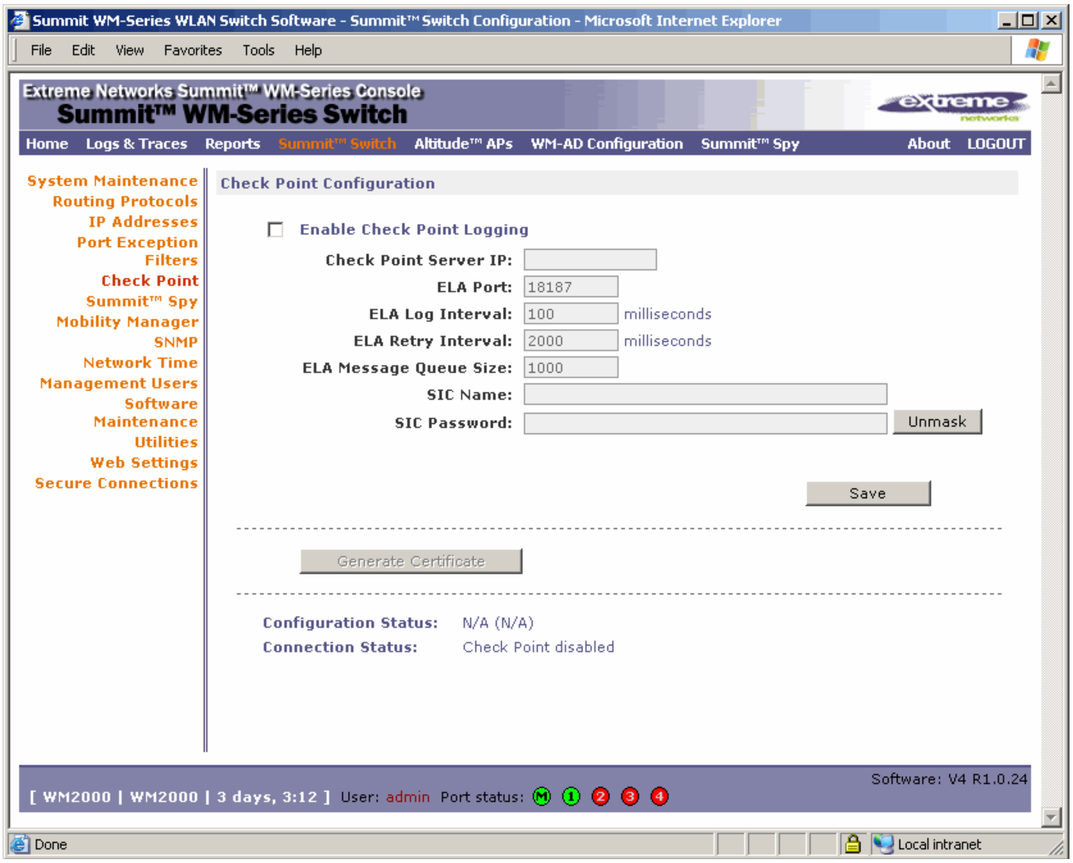
NOTE

Before you set up the Summit WM series switch, you must first create OPSEC objects for Summit WM series switch in the Check Point management software. The name and password you define must also be entered into the Summit WM series switch Check Point configuration screen.

To enable and configure Check Point:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 In the left pane, click **Check Point**. The **Check Point Configuration** screen is displayed.



Check Point Configuration

□ Enable Check Point Logging

Check Point Server IP:

ELA Port: 18187

ELA Log Interval: 100 milliseconds

ELA Retry Interval: 2000 milliseconds

ELA Message Queue Size: 1000

SIC Name:

SIC Password:

Configuration Status: N/A (N/A)

Connection Status: Check Point disabled

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

3 To enable check point logging, select the **Enable Check Point Logging** checkbox.

4 Type the following information:

- **Check Point Server IP** – Specifies the IP address of the ELA Management Station
- **ELA Port** – Specifies the port to use for ELA. The default port is 18187.
- **ELA Log Interval** – Specifies the amount of time (in milliseconds) you want the system to wait before attempting to log once there is a connection between Summit WM series switch and the Check Point gateway. The default is **100** milliseconds.
- **ELA Retry Interval** – Specifies the amount of time (in milliseconds) you want the system to wait before attempting a re-connection between Summit WM series switch and the Check Point gateway. The default is **2000** milliseconds.
- **ELA Message Queue Size** – Specifies the number of messages the log queue holds if the Summit WM series switch and the Check Point gateway become disconnected. The default is **1000** log entries.
- **SIC Name** – Specifies the Secure Internal Communication (SIC) Name, your security-based ID.
- **SIC Password** – Specifies your Secure Internal Communication (SIC) password. You can use the **Unmask** button to display the password.

5 To save your changes, click **Save**.

6 To create the certificate to be sent to the ELA Management Station, click **Generate Certificate** button.

If the certificate is properly generated and the connection with the ELA Management Station is made, the **Connection Status** section displays the following message:

OPSEC Connection OK

If there is an error in generating the certificate or establishing the connection, the **Connection Status** section displays the following message:

OPSEC Connection Error

ELA Management Station events

The events for the ELA Management Station are grouped under Extreme Networks and are mapped as info events and alert events. The alerts include:

- Altitude AP registration and/or authentication failed
- Authentication User Request unsuccessful
- RADIUS server rejected login (Access Rejected)
- An unknown AP has attempted to connect. AP authentication failure.
- A connection request failed to authenticate with the CM messaging server. This may indicate port-scanning of the Summit WM series switch, or a back-door access attempt.
- Unauthorized client attempting to connect

Enabling SNMP

The Summit WM series switch, access points, and WLAN switch software system supports Simple Network Management Protocol (SNMP), Version 1 and 2c. SNMP, a set of protocols for managing complex networks, is used to retrieve Summit WM series switch statistics and configuration information.

SNMP sends messages, called protocol data units (PDUs), to different parts of a network. Devices on the network that are SNMP-compliant, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

MIB support

The Summit WM series switch, access points, and WLAN switch software system accepts SNMP Get commands and generates Trap messages. Support is provided for the retrieval information from the router MIB-II (SNMP_GET) as well as SNMP traps. The supported MIBs include:

- SNMPv2-MIB
- IF-MIB
- IEEE802dot11-MIB
- RFC1213-MIB

NOTE

The Summit WM series switch is not fully compliant with MIB II. For example, esa/IXP ports only provide interface statistics.

The Extreme Networks **Enterprise MIB** includes:

- EXTREME-SUMMIT-WM-MIB.my
- EXTREME-SUMMIT-WM-SMI
- EXTREME-SUMMIT-DOT11-EXTNS-MIB
- EXTREME-SUMMIT-WM-BRANCH-OFFICE-MIB

The MIB is provided for compilation into an external NMS. No support has been provided for automatic device discovery by an external NMS.

The Summit WM series switch is the only point of SNMP access for the entire system. In effect, the Summit WM series switch proxies sets, gets, and alarms from the associated Altitude APs.

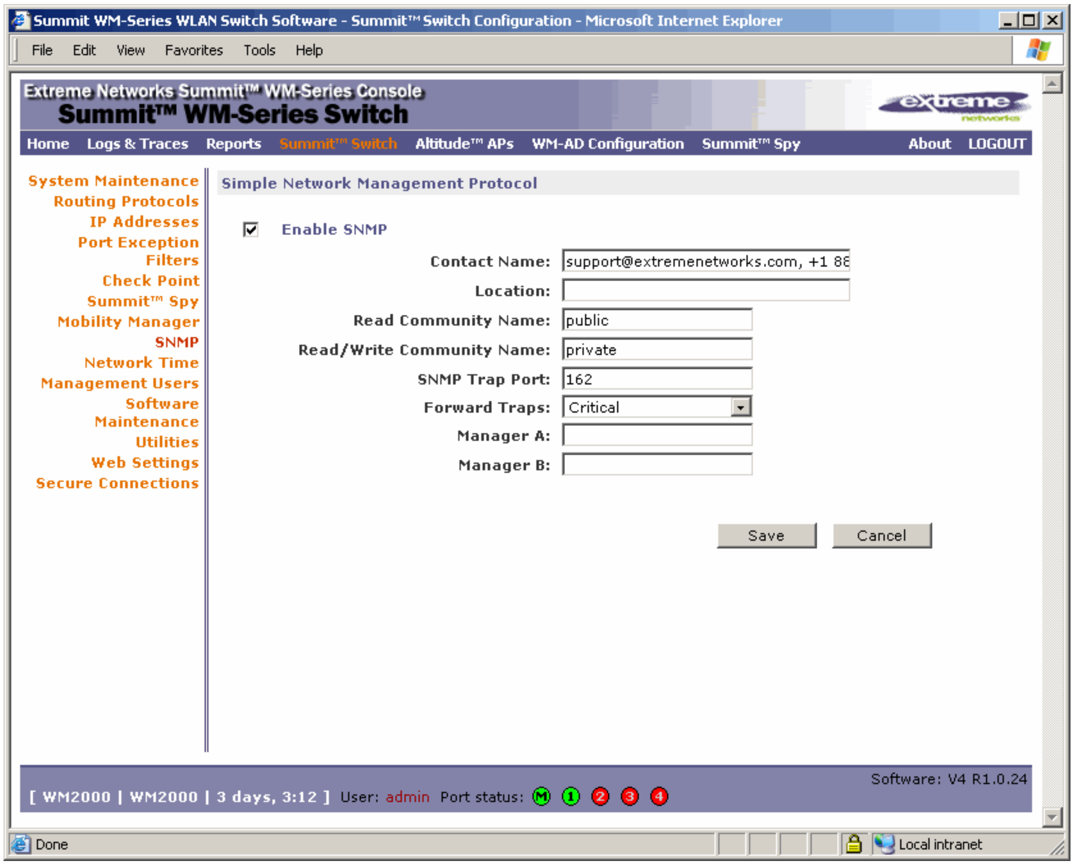
Enabling SNMP on the Summit WM series switch

You can enable SNMP on the Summit WM series switch to retrieve statistics and configuration information.

To enable SNMP Parameters:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 In the left pane, click **SNMP**. The **Simple Network Management Protocol** screen is displayed.



Simple Network Management Protocol

☑ Enable SNMP

Contact Name: support@extremenetworks.com, +1 88

Location:

Read Community Name: public

Read/Write Community Name: private

SNMP Trap Port: 162

Forward Traps: Critical

Manager A:

Manager B:

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

3 Type: the following information:

- **Contact Name** – Specifies the name of SNMP administrator.
- **Location** – Specifies the location of the SNMP administration machine.
- **Read Community Name** – Specifies the community name for users with read privileges.
- **Read/Write Community Name** – Specifies the community name for users with read and write privileges.
- **SNMP Trap Port** – Specifies the destination port for SNMP traps. The industry standard is 162. If left blank, no traps are generated.
- **Forward Traps** – Specifies the security level of the traps to be forwarded. From the drop-down list, select **Informational**, **Minor**, **Major**, or **Critical**.
- **Manager A** – Specifies the IP address of the specific machine on the network where the SNMP traps are monitored.
- **Manager B** – Specifies the IP address of a second machine on the network where the SNMP traps are monitored, if Manager A is not available.

NOTE

For security purposes, it is recommended that you immediately change the Read Community Name (public) and the Read/Write Community Name (private) to names that are less obvious and more secure.

Using controller utilities

You can use Summit WM series switch utilities to test a connection to the target IP address or to record the route through the Internet between your computer and the target IP address.

To test or record IP address connections:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

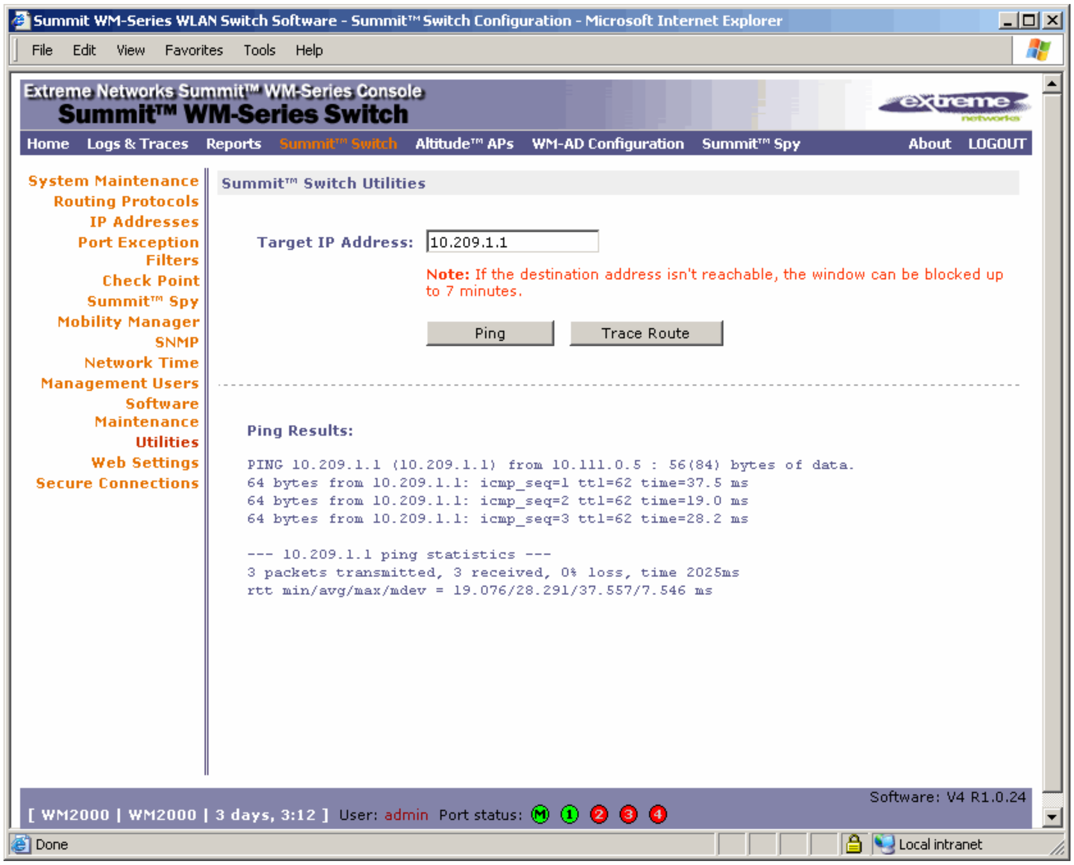
2 In the left pane, click **Utilities**. The **Summit Switch Utilities** screen is displayed.

3 In the **Target IP Address** box, type the IP address of the destination computer.

4 To test a connection to the target IP address, click **Ping**.

5 To record the route through the Internet between your computer and the target IP address, click **Trace Route**.

The following is an example of a screen after clicking the **Trace Route** button.



Summit™ Switch Utilities

Target IP Address: 10.209.1.1

Note: If the destination address isn't reachable, the window can be blocked up to 7 minutes.

Ping Results:

```
PING 10.209.1.1 (10.209.1.1) from 10.111.0.5 : 56(84) bytes of data.
64 bytes from 10.209.1.1: icmp_seq=1 ttl=62 time=37.5 ms
64 bytes from 10.209.1.1: icmp_seq=2 ttl=62 time=19.0 ms
64 bytes from 10.209.1.1: icmp_seq=3 ttl=62 time=28.2 ms

--- 10.209.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% loss, time 2025ms
rtt min/avg/max/mdev = 19.076/28.291/37.557/7.546 ms
```

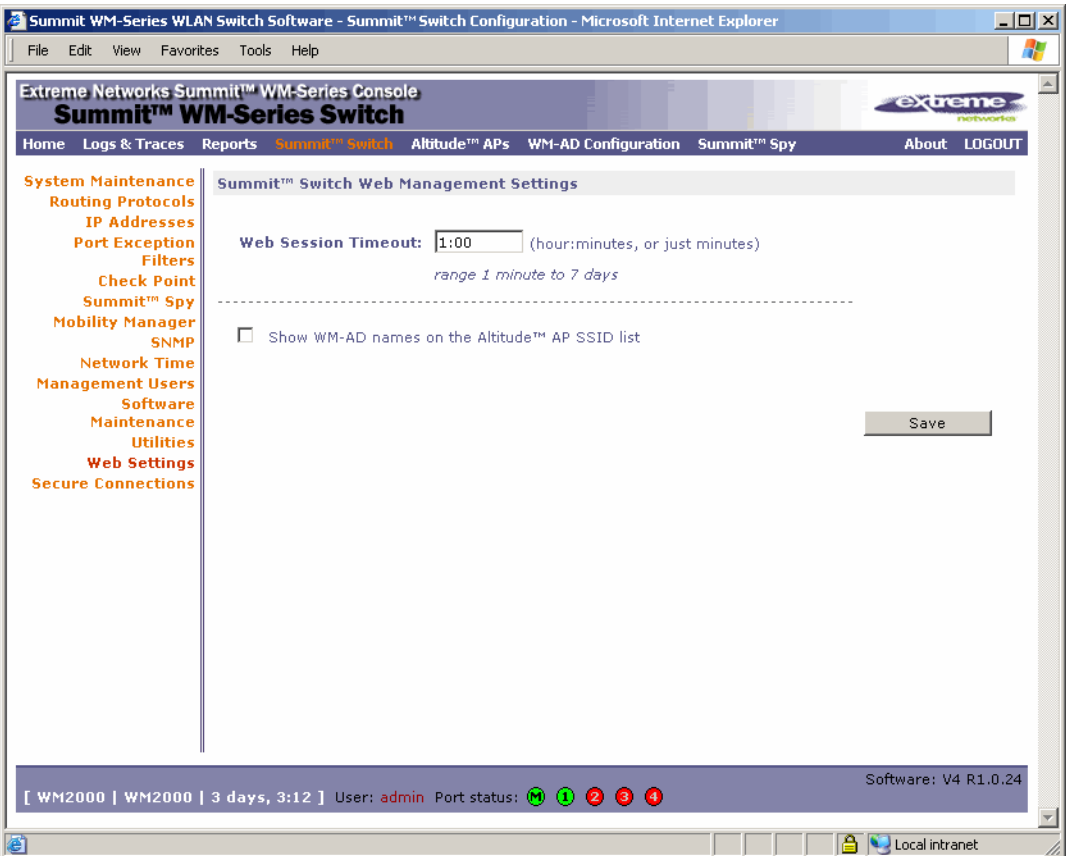
Configuring Web session timeouts

You can configure the time period to allow Web sessions to remain inactive before timing out.

To configure Web session timeouts:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 In the left pane, click **Web Settings**. The **Summit Switch Web Management Settings** screen is displayed.


Summit WM-Series WLAN Switch Software - Summit™ Switch Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Switch
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
System Maintenance
Routing Protocols
IP Addresses
Port Exception Filters
Check Point
Summit™ Spy
Mobility Manager
SNMP
Network Time
Management Users
Software Maintenance
Utilities
Web Settings
Secure Connections
Save
Local intranet

Summit™ Switch Web Management Settings

Web Session Timeout: 1:00 (hour:minutes, or just minutes)

range 1 minute to 7 days

□ Show WM-AD names on the Altitude™ AP SSID list

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

3 In the **Web Session Timeout** box, type the time period to allow the Web session to remain inactive before it times out. This can be entered as hour:minutes, or as minutes. The range is 1 minute to 168 hours.

4 Select the **Show WM-AD names on the Altitude AP SSID list** checkbox to allow the names of the WM-ADs to appear in the SSID list for Altitude APs.

5 To save your settings, click **Save**.

NOTE

Screens that auto-refresh will time out, unless a manual action takes place prior to the end of the timeout period.

7 Working with third-party APs

You can set up the Summit WM series switch to handle wireless device traffic from third-party access points, providing the same policy and network access control. This process requires the following steps:

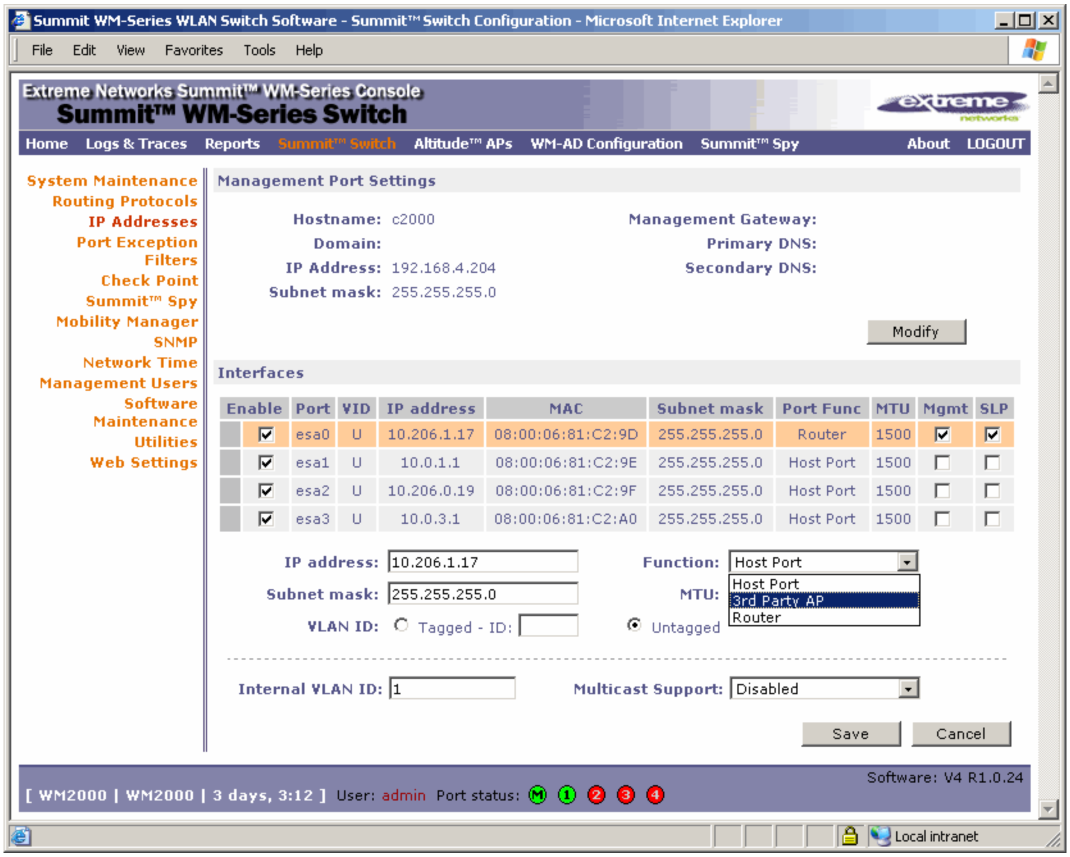
- Step 1 – Define a data port as a third party AP port:
- Step 2 – Define a WM-AD for the third-party AP port:
- Step 3 – Define authentication by Captive Portal and RAD policy for the third-party AP WM-AD:
- Step 4 – Define filtering rules for the third-party APs:

To set up third-party APs:

Step 1 – Define a data port as a third party AP port:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 From the left pane, click **IP Address**. The **Management Port Settings and Interfaces** screen is displayed.



Management Port Settings

Hostname: c2000
Domain:
IP Address: 192.168.4.204
Subnet mask: 255.255.255.0
Management Gateway:
Primary DNS:
Secondary DNS:

Interfaces

Enable	Port	VID	IP address	MAC	Subnet mask	Port Func	MTU	Mgmt	SLP
☑	esa0	U	10.206.1.17	08:00:06:81:C2:9D	255.255.255.0	Router	1500	☑	☑
☑	esa1	U	10.0.1.1	08:00:06:81:C2:9E	255.255.255.0	Host Port	1500	□	□
☑	esa2	U	10.206.0.19	08:00:06:81:C2:9F	255.255.255.0	Host Port	1500	□	□
☑	esa3	U	10.0.3.1	08:00:06:81:C2:A0	255.255.255.0	Host Port	1500	□	□

IP address: 10.206.1.17
Subnet mask: 255.255.255.0
VLAN ID: ○ Tagged - ID: ● Untagged
Function: Host Port
MTU:

Internal VLAN ID: 1
Multicast Support: Disabled

Software: V4 R1.0.24
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

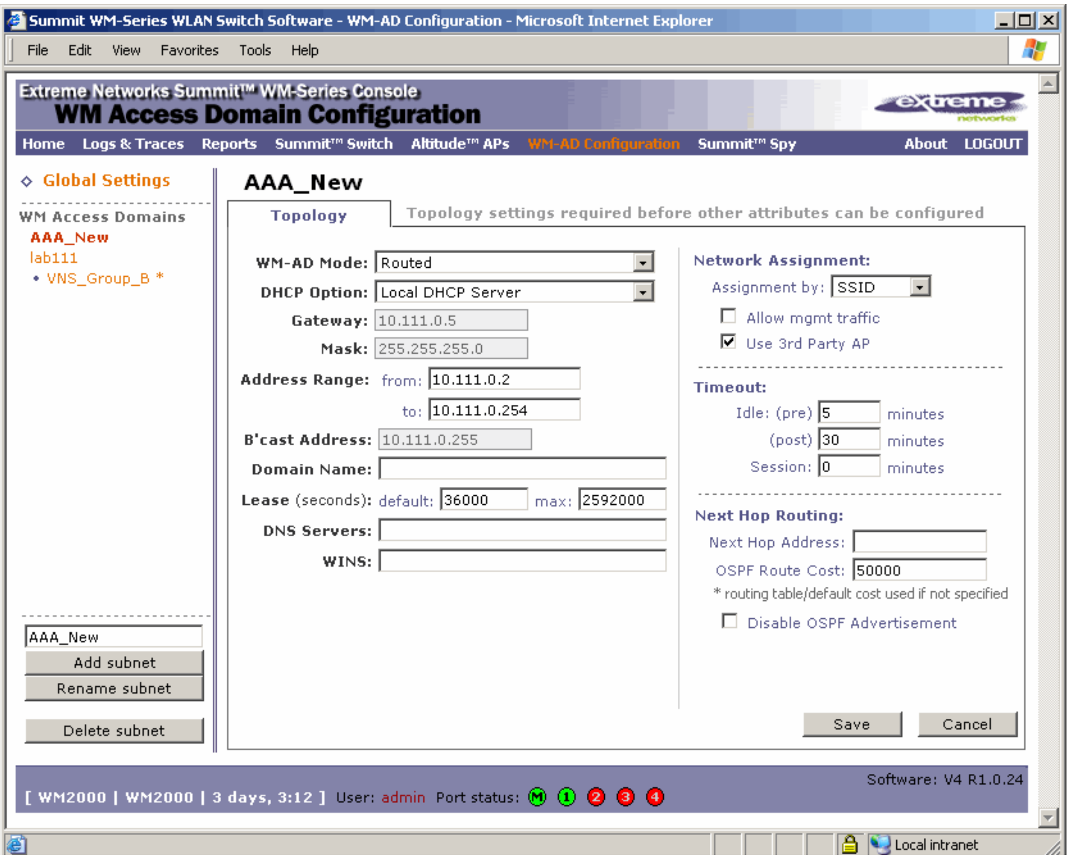
3 Highlight the appropriate port, and in the **Function** box, select **3rd-party AP** from the drop-down list. Make sure that Management Traffic and SLP are disabled for this port.

4 Connect the third-party access point to this port, via a switch.

Step 2 – Define a WM-AD for the third-party AP port:

1 From the main menu, click **WM-AD Configuration**. The WM-AD Configuration screen is displayed.

2 In the left pane, type a name that will identify the new WM-AD in the **Add subnet** box, and then click **Add subnet**. The name is displayed in the **WM Access Domains** list. The **Topology** tab is displayed.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domains
AAA_New
lab111
VNS_Group_B *
Add subnet
Rename subnet
Delete subnet
Topology
Save
Cancel
Local intranet

AAA_New

Topology settings required before other attributes can be configured

WM-AD Mode: Routed

DHCP Option: Local DHCP Server

Gateway: 10.111.0.5

Mask: 255.255.255.0

Address Range: from: 10.111.0.2 to: 10.111.0.254

B'cast Address: 10.111.0.255

Domain Name:

Lease (seconds): default: 36000 max: 2592000

DNS Servers:

WINS:

Network Assignment:

Assignment by: SSID

☐ Allow mgmt traffic

☑ Use 3rd Party AP

Timeout:

Idle: (pre) 5 minutes

(post) 30 minutes

Session: 0 minutes

Next Hop Routing:

Next Hop Address:

OSPF Route Cost: 50000

* routing table/default cost used if not specified

☐ Disable OSPF Advertisement

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

3 In the **Assignment by** drop-down list, click **SSID**.

4 To define a WM-AD for a third-party AP, select the **Use 3rd Party AP** checkbox.

5 Continue configuring your WM-AD as described in "Configuring topology for a WM-AD for Captive Portal" on page 98.

NOTE

Bridge Traffic at AP and MAC-based authentication are not available for Third Party WM-ADs.

Step 3 – Define authentication by Captive Portal and RAD policy for the third-party AP WM-AD:

1 Click the **Auth & Acct** tab.

2 In the **Authentication Configuration** screen, click **Configure Captive Portal Settings**.

3 In the **Captive Portal Settings** screen, define the Captive Portal configuration.

4 Click the **RAD Policy** tab.

5 Define the filter IDs to match those in RADIUS server.

Step 4 – Define filtering rules for the third-party APs:

1 Because the third-party APs are mapped to a physical port, you must define the Exception filters on the physical port, using the Port Exception Filters screen. For more information, see "Configuring filtering rules for a WM-AD" on page 123.

2 Define filtering rules that allow access to other services and protocols on the network such as HTTP, FTP, Telnet, SNMP.

In addition, modify the following functions on the third-party access point:

- Disable the access point's DHCP server, so that the IP address assignment for any wireless device on the AP is from the DHCP server at the Summit WM series switch with WM-AD information.
- Disable the third-party access point's layer-3 IP routing capability and set the access point to work as a layer-2 bridge.

Here are the differences between third-party access points and Altitude APs on the Summit WM series switch, access points, and WLAN switch software system:

- A third-party access point exchanges data with the Summit WM series switch's data port using standard IP over Ethernet protocol. The third-party access points do not support the tunnelling protocol for encapsulation.
- For third-party access points, the WM-AD is mapped to the physical data port and this is the default gateway for mobile units supported by the third-party access points.
- A Summit WM series switch cannot directly control or manage the configuration of a third-party access point.
- Third-party access points are required to broadcast an SSID unique to their segment. This SSID cannot be used by any other WM-AD.
- Roaming from third-party access points to Altitude APs and vice versa is not supported.

8 Working with the Summit WM Series Spy

This chapter describes Summit spy concepts, including:

- Summit spy overview
- Enabling the Analysis and data collector engines
- Running Summit Spy scans
- Analysis engine overview
- Working with Summit spy scan results
- Working with friendly APs
- Viewing the Summit spy list of third-party APs
- Maintaining the Summit spy list of APs
- Viewing the Scanner Status report

Summit spy overview

The Summit spy is a mechanism that assists in the detection of rogue APs. Summit spy functionality does the following:

Altitude AP:

- Runs a radio frequency (RF) scanning task.
- Alternating between scan functions, providing its regular service to the wireless devices on the network.

Summit WM series switch:

- Runs a data collector application that receives and manages the RF scan messages sent by the Altitude AP. RF data collector data includes lists of all connected Altitude APs, third-party APs, and the RF scan information that has been collected from the Altitude APs selected to perform the scan.
- Runs an Analysis Engine that processes the scan data from the data collector through algorithms that make decisions about whether any of the detected APs or clients are rogue APs or are running in an unsecure environment (for example, ad-hoc mode).

NOTE

In a network with more than one Summit WM series switch, it is not necessary for the data collector to be running on the same controller as the Analysis Engine. One controller can be a dedicated Analysis Engine while the other controllers run data collector functionality. No more than one Analysis Engine can be running at a time. You must ensure that the controllers are all routable.

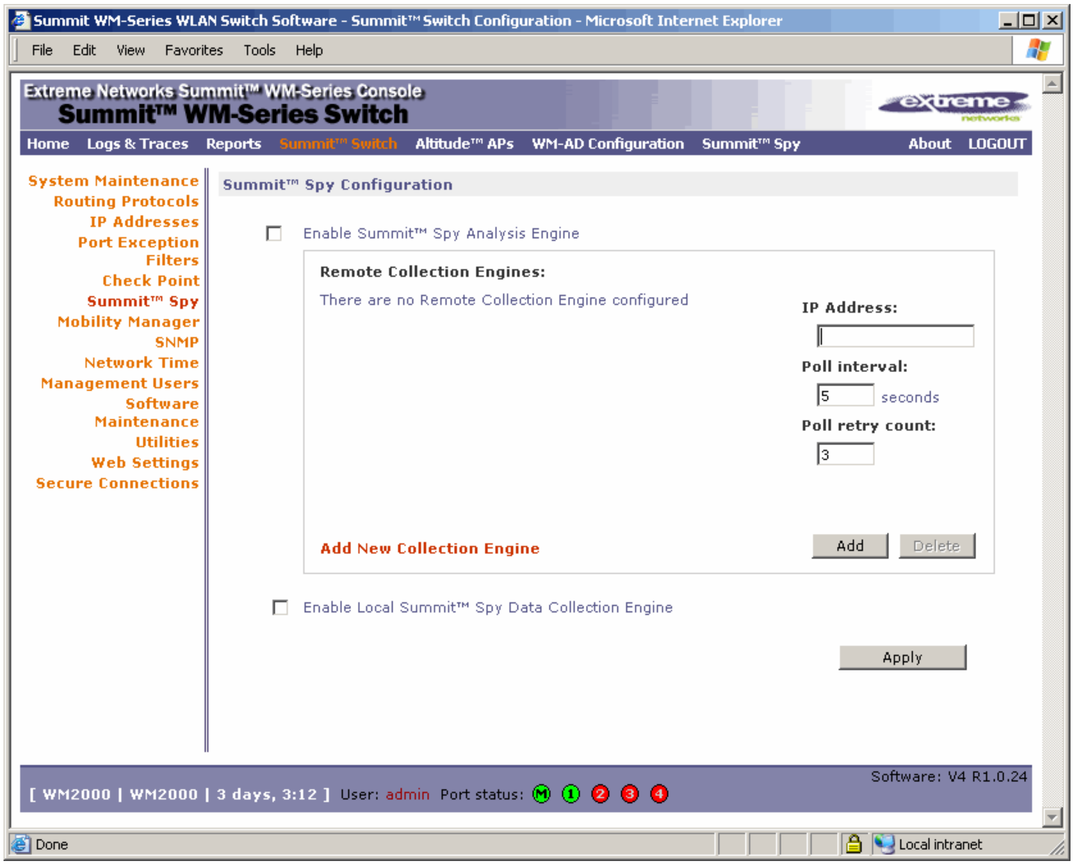
Enabling the Analysis and data collector engines

Before using the Summit spy, you must enable and define the Analysis and data collector engines.

To enable the Analysis engine:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 In the left pane, click **Summit Spy**. The **Summit Spy Configuration** screen is displayed.


Summit WM-Series WLAN Switch Software - Summit™ Switch Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Switch
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
System Maintenance
Routing Protocols
IP Addresses
Port Exception Filters
Check Point
Summit™ Spy
Mobility Manager
SNMP
Network Time
Management Users
Software Maintenance
Utilities
Web Settings
Secure Connections
Summit™ Spy Configuration
Add New Collection Engine
Add
Delete
Apply
Done
Local intranet

□ Enable Summit™ Spy Analysis Engine

Remote Collection Engines:

There are no Remote Collection Engine configured

IP Address:

Poll interval: 5 seconds

Poll retry count: 3

□ Enable Local Summit™ Spy Data Collection Engine

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

3 To enable the Summit Spy Analysis Engine, select the **Enable Summit Spy Analysis Engine** checkbox.

4 To enable the Summit Spy Data Collection Engine on this Summit WM series switch, select the **Enable Local Summit Spy Data Collection Engine** checkbox.

5 To identify the remote RF Data Collector Engine that the Analysis Engine will poll for data, type the IP address of the Summit WM series switch on which the remote Data Collector resides in the **IP Address** box.

6 For the data collection engine:

- In the **Poll interval** box, type (in seconds) the interval that the Analysis Engine will poll the RF Data Collector to maintain connection status. The default is **30** seconds.
- In the **Poll retry count** box, type the number of times the Analysis Engine will attempt to poll the RF Data Collector to maintain connection status, before it stops sending requests. The default is **2** attempts.

7 Click **Add**. The IP address of the Data Collection Engine, with its Poll Interval and Poll Retry parameters is displayed in the list.

NOTE

For each remote RF Data Collection Engine defined here, you must:

> Enable it by selecting the Enable Summit Spy Analysis Engine checkbox on the remote Summit WM series switch

> Ensure that the controllers are routable by whatever means you use (for example, static routes, or OSPF).

8 To add a new collection engine, click **Add Collection Engine**.

9 Repeat steps 4 to 7.

10 To save your changes, click **Apply**.

Running Summit Spy scans

The Summit Spy feature allows you to view the following:

- Scan Groups
- Friendly APs
- Third-party APs
- AP Maintenance

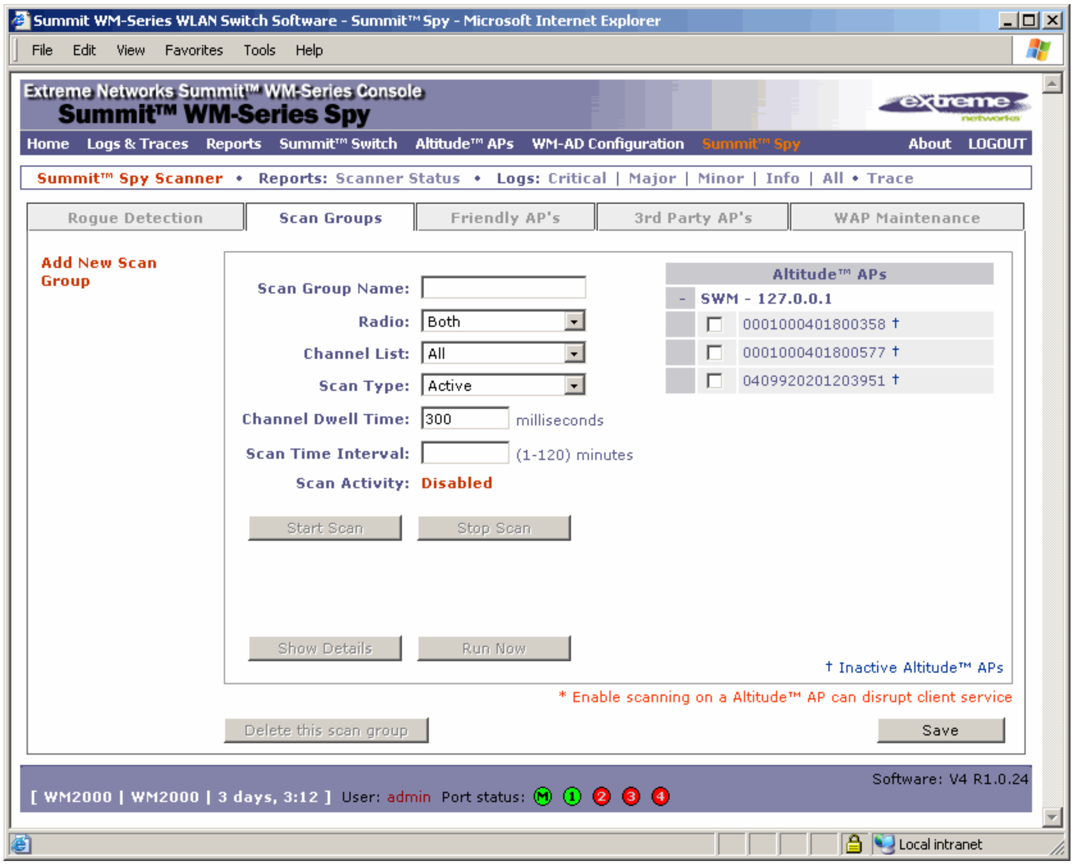
NOTE

A scan will not run on an inactive AP, even though it is displayed as part of the Scan Group. If it becomes active, it will be sent a scan request during the next periodic scan.

To run the Summit Spy scan task mechanism:

1 From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.

2 Click the **Scan Groups** tab.


Summit WM-Series WLAN Switch Software - Summit™ Spy - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Spy
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Summit™ Spy Scanner • Reports: Scanner Status • Logs: Critical | Major | Minor | Info | All • Trace
Rogue Detection Scan Groups Friendly AP's 3rd Party AP's WAP Maintenance
Add New Scan Group
Start Scan Stop Scan
Show Details Run Now
Delete this scan group Save
Local intranet

Scan Group Name:

Radio: Both

Channel List: All

Scan Type: Active

Channel Dwell Time: 300 milliseconds

Scan Time Interval: (1-120) minutes

Scan Activity: Disabled

Altitude™ APs
- SWM - 127.0.0.1
☐ 0001000401800358 †
☐ 0001000401800577 †
☐ 0409920201203951 †

† Inactive Altitude™ APs

* Enable scanning on a Altitude™ AP can disrupt client service

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

3 In the **Scan Group Name** box, type a unique name for this scan group.

4 In the **Altitude APs** list, select the checkbox corresponding to the Altitude APs you want included in the new scan group, which will perform the scan function.

NOTE

An Altitude AP can participate in only one Scan Group at a time. It is recommended that the Scan Groups represent geographical groupings of Altitude APs.

5 In the **Radio** drop-down list, select one of the following:

- **Both** – The a and b/g radios both perform the scan function.
- a – Only the a radio performs the scan function.
- **b/g** – Only the b/g radio performs the scan function.

6 In the **Channel List** drop-down list, select one of the following:

- **All** – Scanning is performed on all channels.
- **Current** – Scanning is performed on only the current channel.

7 In the **Scan Type** drop-down list, select one of the following:

- **Active** – The Altitude AP sends out ProbeRequests and waits for ProbeResponse messages from any access points.

- **Passive** – The Altitude AP listens for 802.11 beacons.

8 In the **Channel Dwell Time** box, type the time (in milliseconds) for the scanner to wait for a response from either 802.11 beacons in passive scanning, or ProbeResponse in active scanning.

9 In the **Scan Time Interval** box, type the time (in minutes) to define the frequency at which an Altitude AP within the Scan Group will initiate a scan of the RF space. The range is from one minute to 120 minutes.

10 To initiate a scan using the periodic scanning parameters defined above, click **Start Scan**.

11 To initiate an immediate scan that will run only once, click **Run Now**.

NOTE

If necessary, you can stop a scan by clicking Stop Scan. A scan must be stopped before modifying any parameters of the Scan Group, or before adding or removing an Altitude AP from a Scan Group.

12 The **Scan Activity** box displays the current state of the scan engine.

13 To view a pop-up report showing the timeline of scan activity and scan results, click **Show Details**.

14 To save your changes, click **Save**.

Analysis engine overview

The Analysis engine relies on a database of known devices on the Summit WM series switch, access points, and WLAN switch software system. The Analysis engine compares the data from the RF Data Collector with the database of known devices.

This database includes the following:

- **Altitude APs** – Registered with any Summit WM series switch with its RF Data Collector enabled and associated with the Analysis Engine on this Summit WM series switch.
- **Third-party APs** – Defined and assigned to a WM-AD.
- **Friendly APs** – A list created in the Summit spy user interface as potential rogue access points are designated by the administrator as Friendly.
- **Wireless devices** – Registered with any Summit WM series switch that has its RF Data Collector enabled and has been associated with the Analysis Engine on this Summit WM series switch.

The Analysis Engine looks for access points with one or more of the following conditions:

- **Unknown MAC address and unknown SSID** (critical alarm)
- **Unknown MAC, with a valid SSID** - a known SSID is being broadcast by the unknown access point (critical alarm)
- **Known MAC, with an unknown SSID** - a rogue may be spoofing a MAC address (critical alarm)
- **Inactive Altitude AP with valid SSID** (critical alarm)
- **Inactive Altitude AP with unknown SSID** (critical alarm)
- **Known Altitude AP with an unknown SSID** (major alarm)
- **In ad-hoc mode** (major alarm)

NOTE

In the current release, there is no capability to initiate a DoS attack on the detected rogue access point. Containment of a detected rogue requires an inspection of the geographical location of its Scan Group area, where its RF activity has been found.

Working with Summit spy scan results

When viewing the Summit spy scan results you can delete all or selected Access Points from the scan results. You can also add Access Points from the scan results to the **Friendly AP** list.

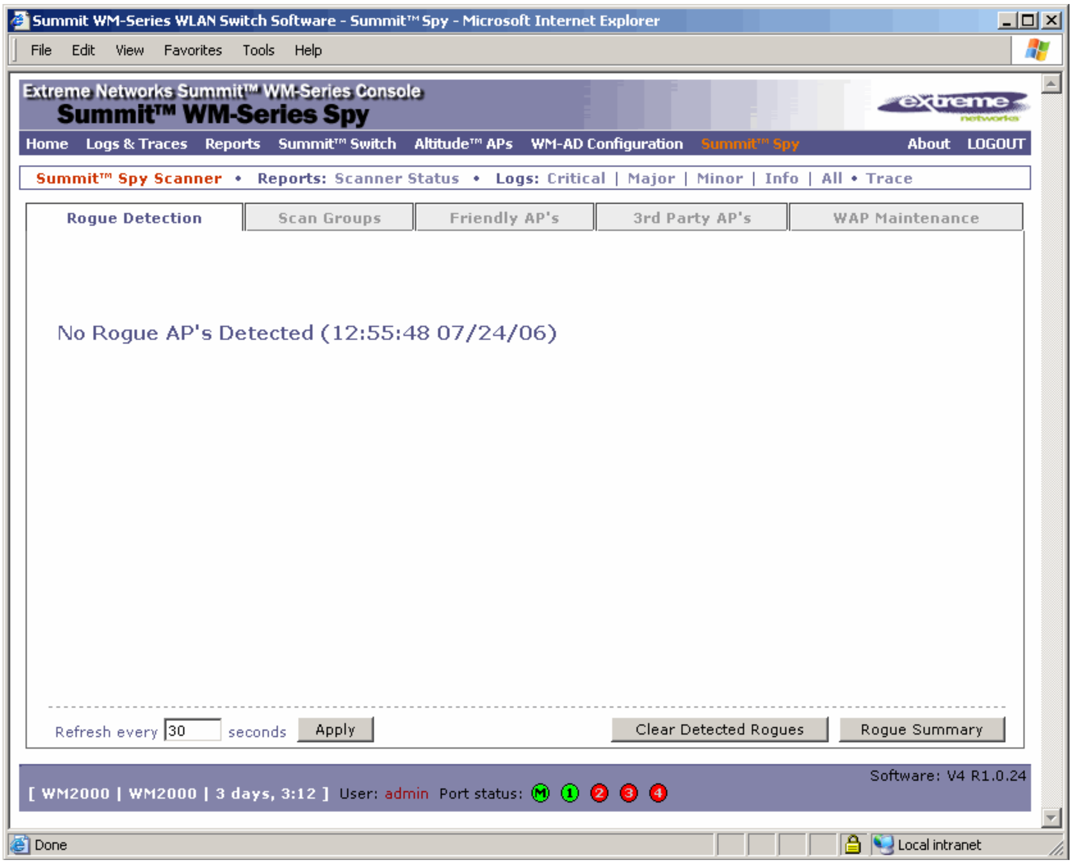
To view Summit Spy scan results:

1 From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.

2 Click the **Rogue Detection** tab.

3 To modify the screen's refresh rate, type a time (in seconds) in the **Refresh every __ seconds** box.

4 Click **Apply**. The new refresh rate is applied.



No Rogue AP's Detected (12:55:48 07/24/06)

Refresh every 30 seconds

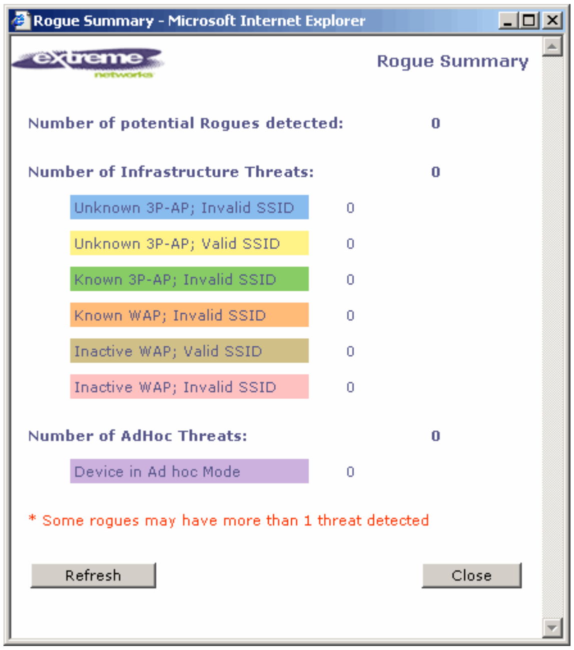
[WM2000 | WM2000 | 3 days, 3:12] User: admin

Software: V4 R1.0.24

Summit WM-Series WLAN Switch Software - Summit™ Spy - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Spy
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Summit™ Spy Scanner • Reports: Scanner Status • Logs: Critical | Major | Minor | Info | All • Trace
Rogue Detection
Scan Groups
Friendly AP's
3rd Party AP's
WAP Maintenance
Apply
Clear Detected Rogues
Rogue Summary
Port status: M 1 2 3 4
Done
Local intranet

5 To view the Rogue Summary report, click **Rogue Summary**. The Rogue Summary report is displayed in a pop-up window.

6 To clear all detected rogue devices from the list, click **Clear Detected Rogues**.



Rogue Summary

Number of potential Rogues detected: 0

Number of Infrastructure Threats: 0

Unknown 3P-AP; Invalid SSID	0
Unknown 3P-AP; Valid SSID	0
Known 3P-AP; Invalid SSID	0
Known WAP; Invalid SSID	0
Inactive WAP; Valid SSID	0
Inactive WAP; Invalid SSID	0

Number of AdHoc Threats: 0

Device in Ad hoc Mode	0

* Some rogues may have more than 1 threat detected

NOTE

To avoid the Summit spy's database becoming too large, it is recommended that you either delete Rogue APs or add them to the Friendly APs list, rather than leaving them in the Rogue list.

To add an AP from the Summit spy scan results to the list of friendly APs:

1 From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.

2 Click the **Rogue Detection** tab.

3 To add an Altitude AP to the **Friendly APs** list, click **Add to Friendly List**. The AP is removed from this list and is displayed in the **Friendly AP Definitions** section of the **Friendly AP's** tab.

To delete an AP from the Summit spy scan results:

1 From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.

2 Click the **Rogue Detection** tab.

3 To delete a specific AP from the Summit spy scan results, click the corresponding **Delete** button. The AP is removed from the list.

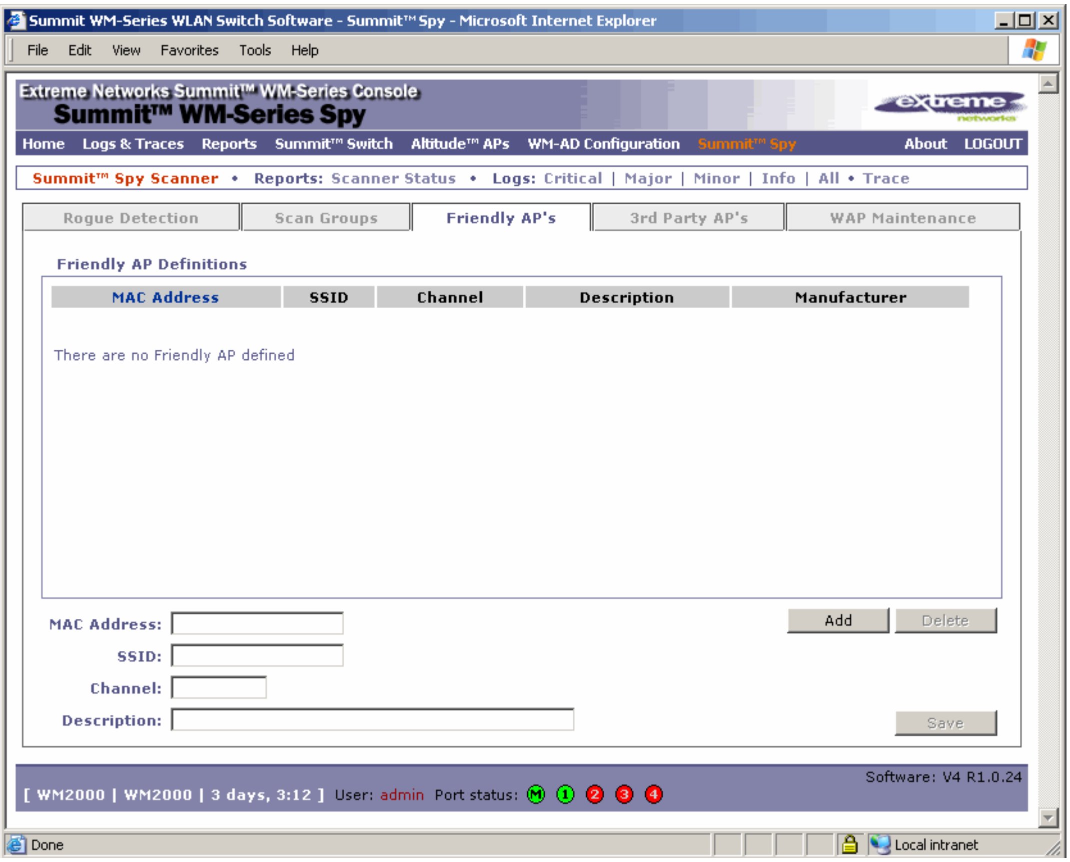
4 To clear all rogue access points from the Summit spy scan results, click **Clear Detected Rogues**. All APs are removed from the list.

Working with friendly APs

To view the friendly APs:

1 From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.

2 Click the **Friendly AP's** tab.


Summit WM-Series WLAN Switch Software - Summit™ Spy - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Spy
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Summit™ Spy Scanner • Reports: Scanner Status • Logs: Critical | Major | Minor | Info | All • Trace
Rogue Detection
Scan Groups
Friendly AP's
3rd Party AP's
WAP Maintenance
Friendly AP Definitions
MAC Address
SSID
Channel
Description
Manufacturer
MAC Address:
SSID:
Channel:
Description:
Add
Delete
Save
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4
Software: V4 R1.0.24
Done
Local intranet

There are no Friendly AP defined

To add friendly APs manually:

1 From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.

2 Click the **Friendly AP's** tab.

3 To add friendly access points manually to the **Friendly AP Definitions** list, type the following:

- MAC Address – Specifies the MAC address for the friendly AP
- SSID – Specifies the SSID for the friendly AP
- Channel – Specifies the current operating channel for the friendly AP
- **Description** – Specifies a brief description for the friendly AP

4 Click **Add**. The new access point is displayed in the list above.

To delete a friendly AP:

1 From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.

2 Click the **Friendly AP's** tab.

3 To select an access point from the **Friendly AP Definitions** list to delete, click it.

4 Click **Delete**. The selected access point is removed from the **Friendly AP Definitions** list.

5 To save your changes, click **Save**.

To modify a friendly AP:

1 From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.

2 Click the **Friendly AP's** tab.

3 To select an access point from the **Friendly AP Definitions** list to modify, click it.

4 Modify the access point by making the appropriate changes.

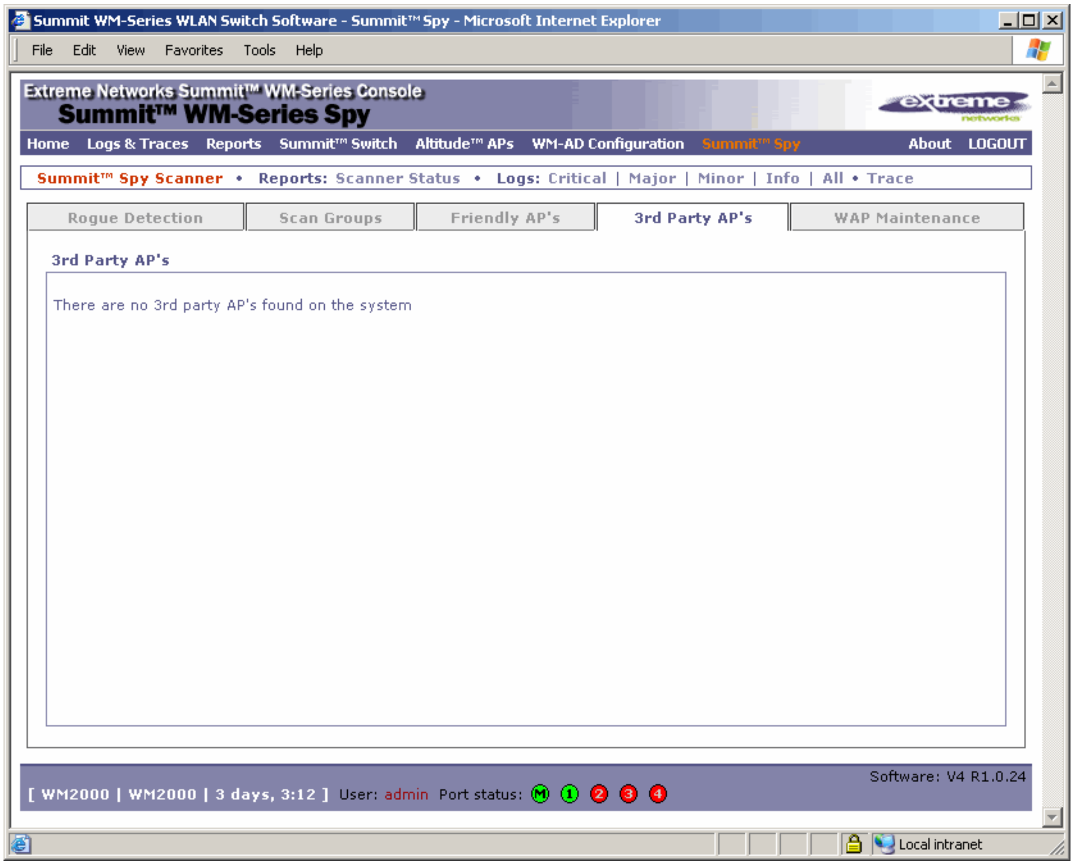
5 To save your changes, click **Save**.

Viewing the Summit spy list of third-party APs

To view known third-party access points connected to local/remote RF data collectors:

1 From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.

2 Click the **3rd Party AP's** tab.


Summit WM-Series WLAN Switch Software - Summit™ Spy - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Spy
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Summit™ Spy Scanner • Reports: Scanner Status • Logs: Critical | Major | Minor | Info | All • Trace
Rogue Detection Scan Groups Friendly AP's 3rd Party AP's WAP Maintenance
Software: V4 R1.0.24
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4
Local intranet

3rd Party AP's

There are no 3rd party AP's found on the system

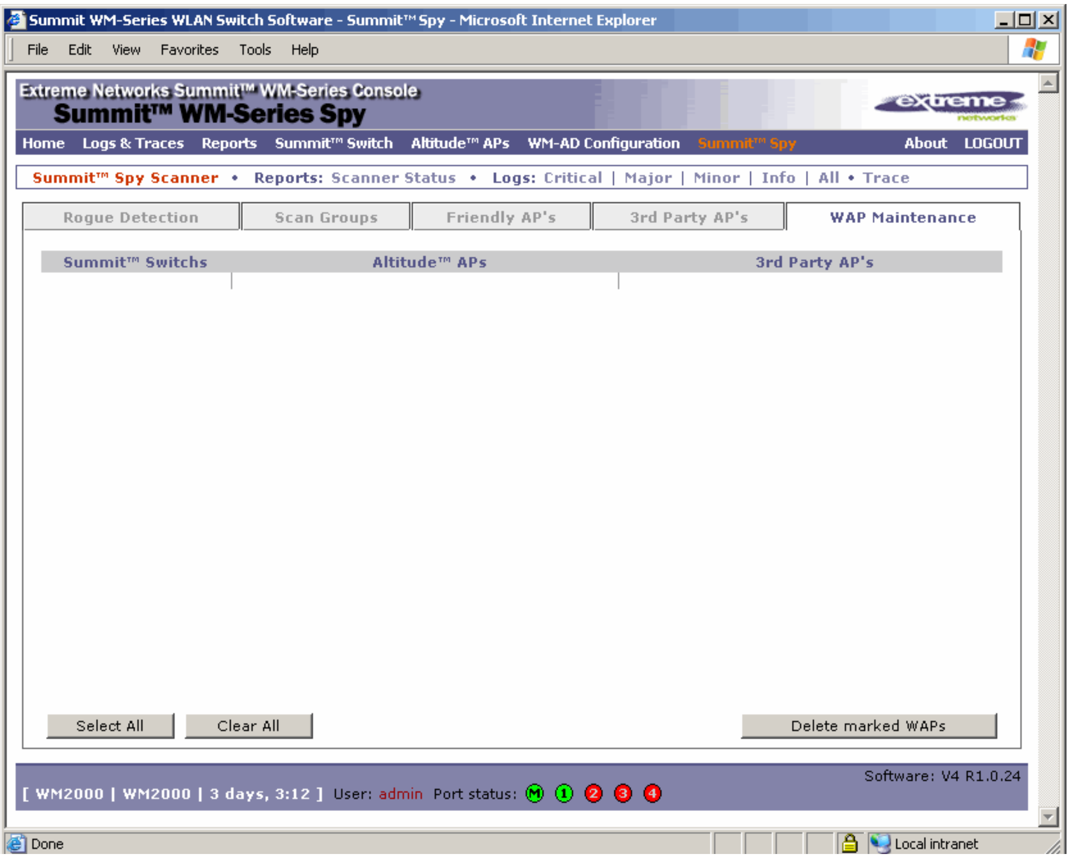
Maintaining the Summit spy list of APs

To maintain the Altitude APs:

1 From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.

2 Click the **WAP Maintenance** tab. Inactive APs and known third-party APs are displayed.

3 Select the applicable APs.


Summit WM-Series WLAN Switch Software - Summit™ Spy - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Spy
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Summit™ Spy Scanner • Reports: Scanner Status • Logs: Critical | Major | Minor | Info | All • Trace
Rogue Detection
Scan Groups
Friendly AP's
3rd Party AP's
WAP Maintenance
Summit™ Switchs
Altitude™ APs
3rd Party AP's
Select All
Clear All
Delete marked WAPs
Software: V4 R1.0.24
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4
Done
Local intranet

4 To delete the selected APs, click **Delete marked WAPs**.

NOTE

The selected APs are deleted from the Summit spy database, not from the Summit WM series switch database. You can delete the APs from the Summit WM series switch database after you delete them from the Altitude AP Configuration Access Approval screen of the corresponding RF Data Collector Engine. You can also delete the selected third-party APs if they are removed from the corresponding WM-AD in the RF Collector Engine, or if that WM-AD has been deleted from the WM-AD list.

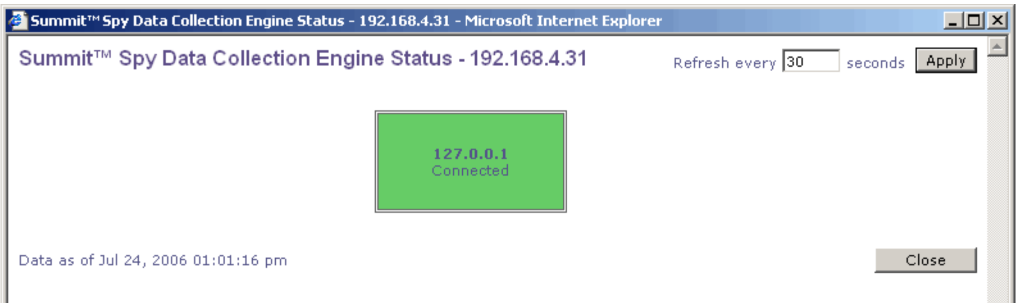
Viewing the Scanner Status report

When the Summit spy is enabled, you can view a report on the connection status of the RF Data Collector Engines with the Analysis Engine.

To view the Summit spy scanner engine status display:

1 From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.

2 Click the **Scanner Status** link. The Scanner Status report is displayed, as shown in the example below.


Summit™ Spy Data Collection Engine Status - 192.168.4.31 - Microsoft Internet Explorer

Summit™ Spy Data Collection Engine Status - 192.168.4.31

Refresh every 30 seconds

127.0.0.1
Connected

Data as of Jul 24, 2006 01:01:16 pm

The boxes display the IP address of the Data Collector engine. The status of the Data Collector engine is indicated by one of the following colors:

- **Green** – The Analysis Engine has connection with the Data Collector on that Summit WM series switch.
- **Yellow** – The Analysis Engine has connected to the communication system of the other controller, but has not synchronized with the Data Collector. Ensure that the Data Collector is running on the remote controller.
- **Red** – The Analysis Engine is aware of the Data Collector and attempting connection.

If no box is displayed, the Analysis Engine is not attempting to connect with that Data Collector Engine.

NOTE

If the box is displayed red and remains red, ensure your IP address is correctly set up to point to an active controller. If the box remains yellow, ensure the Data Collector is running on the remote controller.

9 Working with reports and displays

This chapter describes the various reports and displays available in the Summit WM series switch, access points, and WLAN switch software system.

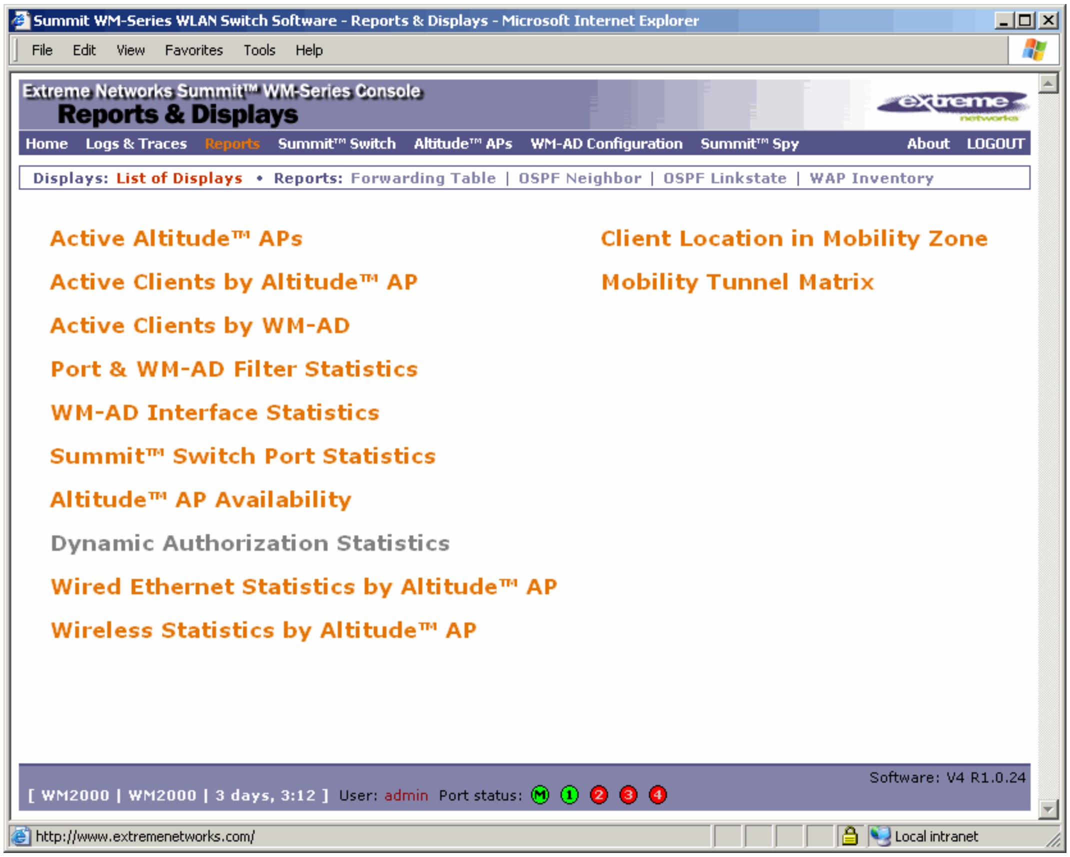
Viewing the displays

The following displays are available in the Summit WM series switch, access points, and WLAN switch software system:

- Active Altitude APs
- Active Clients by Altitude AP
- Active Clients by WM-AD
- Port & WM-AD Filter Statistics
- WM-AD Interface Statistics
- Summit Switch Port Statistics
- Altitude AP Availability
- Wired Ethernet Statistics by Altitude AP
- Wireless Statistics by Altitude AP
- Client Location in Mobility Zone
- Mobility Tunnel Matrix

To view reports and displays:

1 From the main menu, click **Reports & Displays**. The **Summit Reports & Displays** screen is displayed.


Summit WM-Series WLAN Switch Software - Reports & Displays - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Reports & Displays
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Displays: List of Displays • Reports: Forwarding Table | OSPF Neighbor | OSPF Linkstate | WAP Inventory
Software: V4 R1.0.24
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4
http://www.extremenetworks.com/
Local intranet

Active Altitude™ APs

Active Clients by Altitude™ AP

Active Clients by WM-AD

Port & WM-AD Filter Statistics

WM-AD Interface Statistics

Summit™ Switch Port Statistics

Altitude™ AP Availability

Dynamic Authorization Statistics

Wired Ethernet Statistics by Altitude™ AP

Wireless Statistics by Altitude™ AP

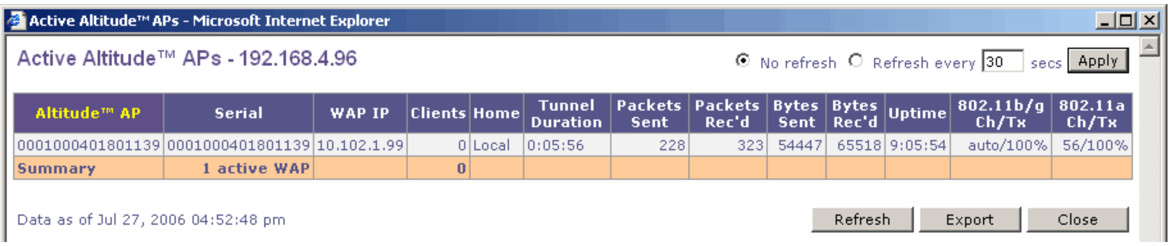
Client Location in Mobility Zone

Mobility Tunnel Matrix

NOTE

The two displays on the right-hand side of the screen only appear if the mobility manager function has been enabled for the controller.

2 In the **List of Displays**, click the display you want to view (some examples will follow):


Active Altitude™ APs - Microsoft Internet Explorer
● No refresh ○ Refresh every 30 secs Apply
Refresh Export Close

Active Altitude™ APs - 192.168.4.96

Altitude™ AP	Serial	WAP IP	Clients	Home	Tunnel Duration	Packets Sent	Packets Rec'd	Bytes Sent	Bytes Rec'd	Uptime	802.11b/g Ch/Tx	802.11a Ch/Tx
0001000401801139	0001000401801139	10.102.1.99	0	Local	0:05:56	228	323	54447	65518	9:05:54	auto/100%	56/100%
Summary	1 active WAP		0									

Data as of Jul 27, 2006 04:52:48 pm

NOTE

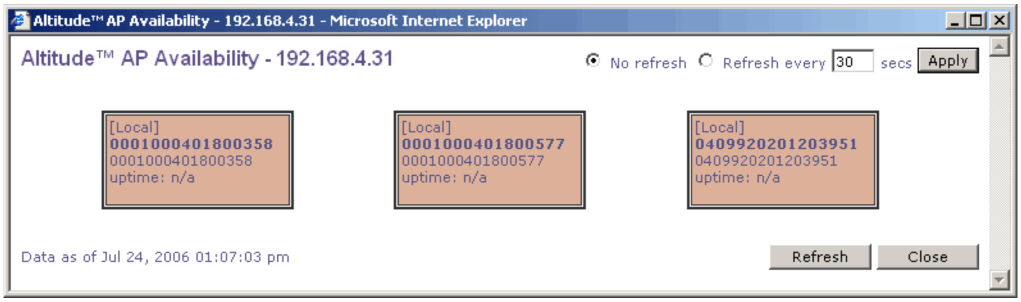
Statistics are expressed in relation to the AP. Therefore, Packets Sent means the AP has sent that data to a client and Packets Rec'd means the AP has received packets from a client.

Viewing the Altitude AP availability display

This display reports the active connection state of an Altitude AP (availability to the Summit WM series switch for service). Depending on the state of the Altitude AP, the following is displayed:

Green – Altitude AP is configured on the Summit WM series switch and is presently connected.

Red – Altitude AP is configured on the Summit WM series switch but is presently not connected (not available to service this Summit WM series switch).



Altitude™ AP Availability - 192.168.4.31 - Microsoft Internet Explorer

Altitude™ AP Availability - 192.168.4.31

● No refresh ○ Refresh every 30 secs

[Local]
0001000401800358
0001000401800358
uptime: n/a

[Local]
0001000401800577
0001000401800577
uptime: n/a

[Local]
0409920201203951
0409920201203951
uptime: n/a

Data as of Jul 24, 2006 01:07:03 pm

In normal operations, when the Summit WM series switch **Availability** feature is enabled, the local Altitude APs are green, and the foreign Altitude APs are red. If the other Summit WM series switch fails, and the foreign Altitude APs connect to the current Summit WM series switch, the display will show all Altitude APs as green. If the Altitude APs are not connected they show up as red.

Viewing statistics for Altitude APs

Two displays are snapshots of activity at that point in time on a selected Altitude AP:

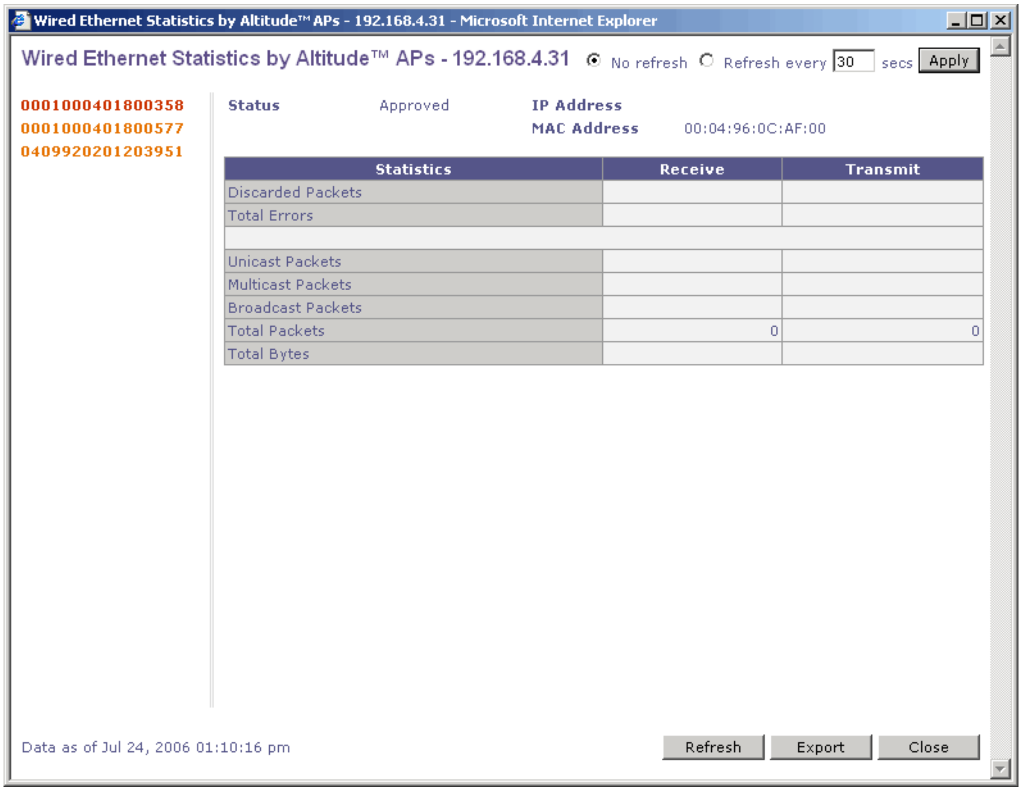
- Wired Ethernet Statistics by Altitude AP
- Wireless Statistics by Altitude AP

The statistics displayed are those defined in the 802.11 MIB, in the IEEE 802.11 standard.

To view wired Ethernet statistics by Altitude AP:

1 From the main menu, click **Reports & Displays**. The **Summit Reports & Displays** screen is displayed.

2 Click the **Wired Ethernet Statistics by Altitude AP** display option. The **Wired Ethernet Statistics by Altitude APs** display opens in a new browser window.



Wired Ethernet Statistics by Altitude™ APs - 192.168.4.31 - Microsoft Internet Explorer

Wired Ethernet Statistics by Altitude™ APs - 192.168.4.31 ● No refresh ○ Refresh every 30 secs Apply

0001000401800358
0001000401800577
0409920201203951

Status Approved IP Address
MAC Address 00:04:96:0C:AF:00

Statistics	Receive	Transmit
Discarded Packets		
Total Errors		
Unicast Packets		
Multicast Packets		
Broadcast Packets		
Total Packets	0	0
Total Bytes		

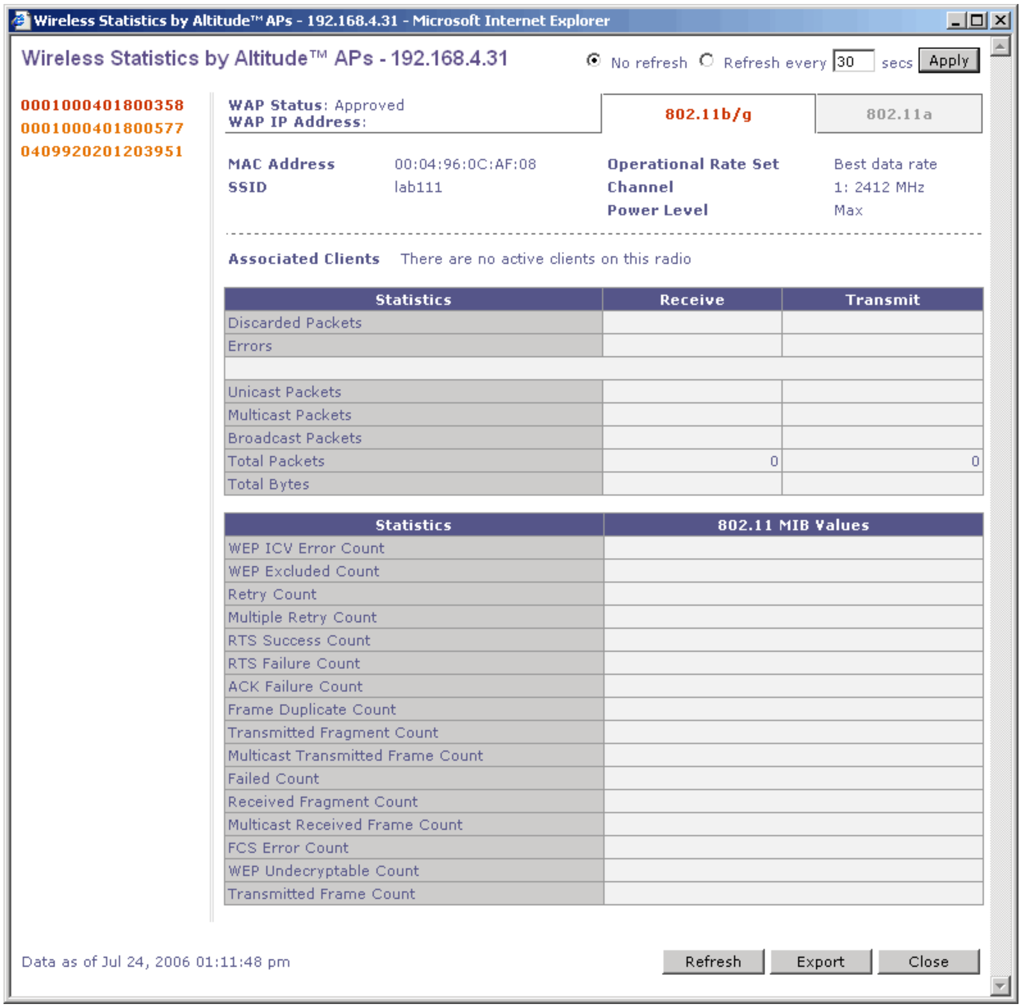
Data as of Jul 24, 2006 01:10:16 pm

3 In the **Wired Ethernet Statistics by Altitude APs** display, click a registered Altitude AP to display its information.

To view Wireless Statistics by Altitude AP:

1 From the main menu, click **Reports & Displays**. The **Summit Reports & Displays** screen is displayed.

2 Click the **Wireless Statistics by Altitude AP** display option. The **Wireless Statistics by Altitude APs** display opens in a new browser window.


Wireless Statistics by Altitude™ APs - 192.168.4.31 - Microsoft Internet Explorer

Wireless Statistics by Altitude™ APs - 192.168.4.31

● No refresh ○ Refresh every 30 secs Apply

0001000401800358
0001000401800577
0409920201203951

WAP Status: Approved
WAP IP Address:

802.11b/g | 802.11a

MAC Address	00:04:96:0C:AF:08	**Operational Rate Set**	Best data rate
SSID	lab111	**Channel**	1: 2412 MHz
		Power Level	Max

Associated Clients There are no active clients on this radio

Statistics	Receive	Transmit
Discarded Packets		
Errors		
Unicast Packets		
Multicast Packets		
Broadcast Packets		
Total Packets	0	0
Total Bytes		

Statistics	802.11 MIB Values
WEP ICV Error Count	
WEP Excluded Count	
Retry Count	
Multiple Retry Count	
RTS Success Count	
RTS Failure Count	
ACK Failure Count	
Frame Duplicate Count	
Transmitted Fragment Count	
Multicast Transmitted Frame Count	
Failed Count	
Received Fragment Count	
Multicast Received Frame Count	
FCS Error Count	
WEP Undecryptable Count	
Transmitted Frame Count	

Data as of Jul 24, 2006 01:11:48 pm

3 In the **Wired Statistics by Altitude APs** display, click a registered Altitude AP to display its information.

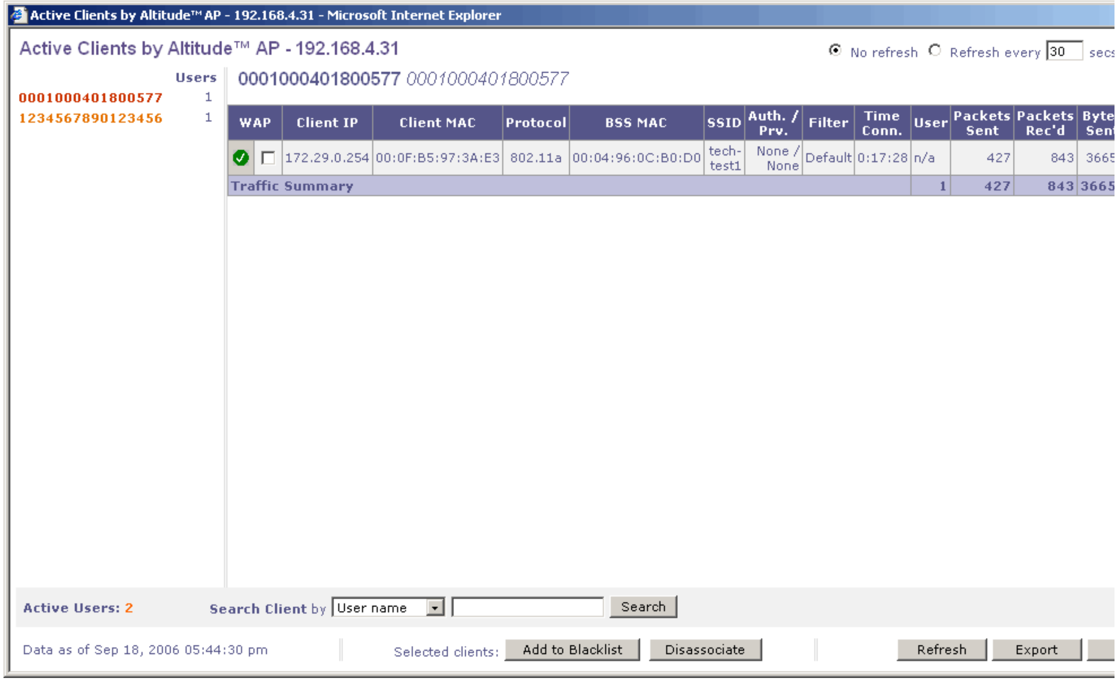
4 Click the appropriate tab to display information for each radio on the Altitude AP.

5 To view information on selected associated clients, click **View Client**. The **Associated Clients** display opens in a new browser window.

To view Active Clients by Altitude AP statistics:

1 From the main menu, click **Reports & Displays**. The **Summit Reports & Displays** screen is displayed.

2 Click the **Active Clients by Altitude APs** display option. The **Active Clients by Altitude APs** display opens in a new browser window.



Active Clients by Altitude™ AP - 192.168.4.31 - Microsoft Internet Explorer

Active Clients by Altitude™ AP - 192.168.4.31

● No refresh ○ Refresh every 30 secs

	Users
0001000401800577	1
1234567890123456	1

0001000401800577 *0001000401800577*

WAP		Client IP	Client MAC	Protocol	BSS MAC	SSID	Auth. / Prv.	Filter	Time Conn.	User	Packets Sent	Packets Rec'd	Byte Sen
✓	□	172.29.0.254	00:0F:B5:97:3A:E3	802.11a	00:04:96:0C:B0:D0	tech-test1	None / None	Default	0:17:28	n/a	427	843	3665
Traffic Summary										1	427	843	3665

Active Users: 2

Search Client by User name

Data as of Sep 18, 2006 05:44:30 pm

Selected clients:

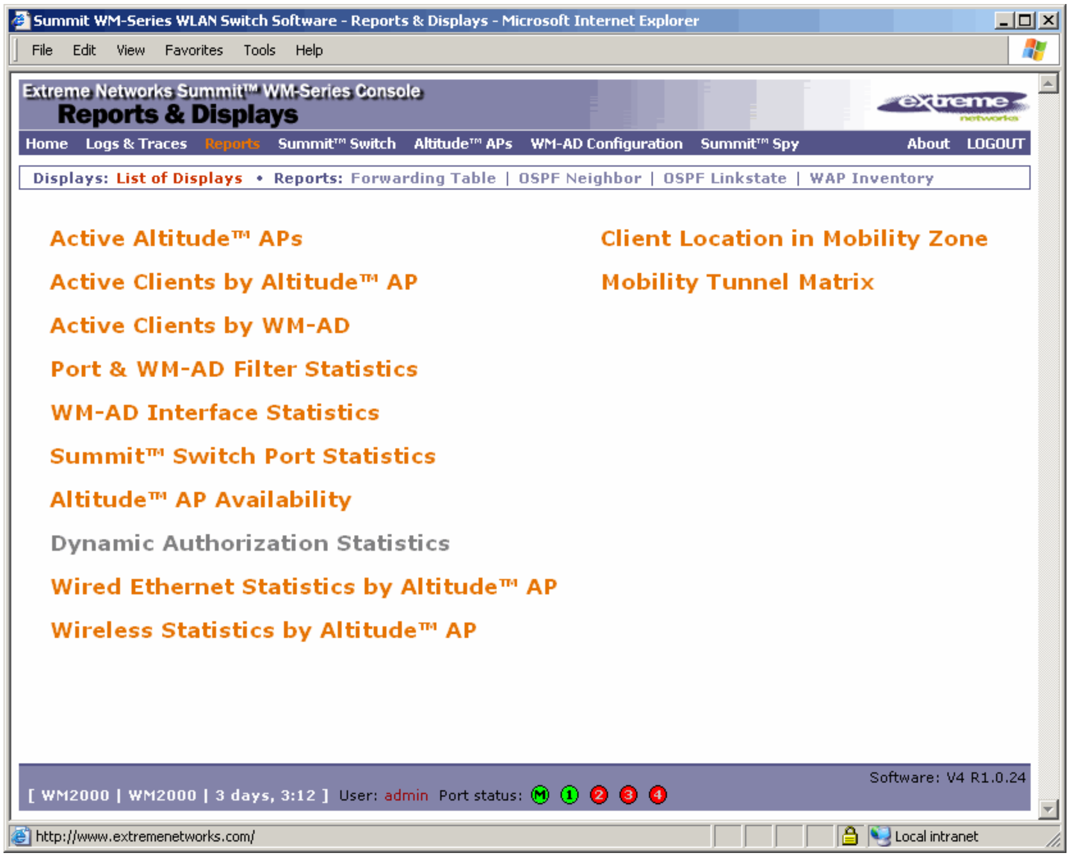
- Statistics are expressed in respect of the AP. Therefore, **Packets Sent** means the AP has sent that data to a client and **Packets Rec'd** means the AP has received packets from a client.
- If the client is authenticated, a green check mark icon is displayed in the first column of the display.
- **Time Conn** is the length of time that a client has been on the system, not just on an AP. If the client roams from one AP to another, the session stays, therefore **Time Conn** does not reset.
- A client is displayed as soon as the client connects (or after refresh of screen). The client disappears as soon as it times out.

Viewing displays for the mobility manager

When a Summit WM series switch has been configured as a mobility manager, two additional displays appear as options in the **Summit Reports & Displays** screen:

- **Client Location in Mobility Zone** – Displays the active wireless clients and their status

- **Mobility Tunnel Matrix** – Displays a cross-connection view of the state of inter-controller tunnels, as well as relative loading for user distribution across the mobility domain


Summit WM-Series WLAN Switch Software - Reports & Displays - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Reports & Displays
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Displays: List of Displays • Reports: Forwarding Table | OSPF Neighbor | OSPF Linkstate | WAP Inventory
Active Altitude™ APs
Active Clients by Altitude™ AP
Active Clients by WM-AD
Port & WM-AD Filter Statistics
WM-AD Interface Statistics
Summit™ Switch Port Statistics
Altitude™ AP Availability
Dynamic Authorization Statistics
Wired Ethernet Statistics by Altitude™ AP
Wireless Statistics by Altitude™ AP
Client Location in Mobility Zone
Mobility Tunnel Matrix
Software: V4 R1.0.24
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4
http://www.extremenetworks.com/
Local intranet

To view mobility manager displays:

1 From the main menu, click **Reports & Displays**. The **Summit Reports & Displays** screen is displayed.

2 Click the appropriate mobility manager display:

   - Client Location in Mobility Zone
   - Mobility Tunnel Matrix

The colored status indicates the following:

- **Green** – The mobility manager is in communication with an agent and the data tunnel has been successfully established.
- **Yellow** – The mobility manager is in communication with an agent but the data tunnel is not yet successfully established.
- **Red** – The mobility manager is not in communication with an agent and there is no data tunnel.

Client Location in Mobility Zone

You can do the following:

- Sort this display by home or foreign controller

- Search for a client by MAC address, user name, or IP address, and typing the search criteria in the box
- Define the refresh rates for this display
- Export this information as an xml file

Mobility Tunnel Matrix

- Provides connectivity matrix of mobility state
- Provides a view of:
  - Tunnel state
  - If a tunnel between controllers is reported down, it is highlighted in red
  - If only a control tunnel is present, it is highlighted in yellow
  - If data and control tunnels are fully established, it is highlighted in green
  - Tunnel Uptime
  - Number of clients roamed (Mobility loading)
  - Local controller loading
  - Mobility membership list

A Summit WM series switch is only removed from the mobility matrix if it is explicitly removed by the administrator from the Mobility permission list. If a particular link between controllers, or the controller is down, the corresponding matrix connections are identified in red color to identify the link.

The Active Clients by WM-AD report for the controller on which the user is home (home controller) will display the known user characteristics (IP, statistics, etc.). On the foreign controller, the Clients by WM-AD report does not show users that have roamed from other controllers, since the users remain associated with the home controller's WM-AD.

The Active Clients by AP report on each controller will show both the loading of local and foreign users (users roamed from other controllers) that are taking resources on the AP

NOTE

The statistics from the mobility manager are updated every thirty seconds, regardless of the refresh period for the displays.

Viewing reports

The following reports are available in the Summit WM series switch, access points, and WLAN switch software system:

- Forwarding Table (routes defined in the Summit WM series switch Routing Protocols screen)
- OSPF Neighbor (if OSPF is enabled in the Routing Protocols screen)
- OSPF Linkstate (if OSPF is enabled in the Routing Protocols screen)
- AP Inventory (a consolidated summary of Altitude AP setup)

To view reports:

1 From the main menu, click **Reports & Displays**. The **Reports & Displays** screen is displayed.

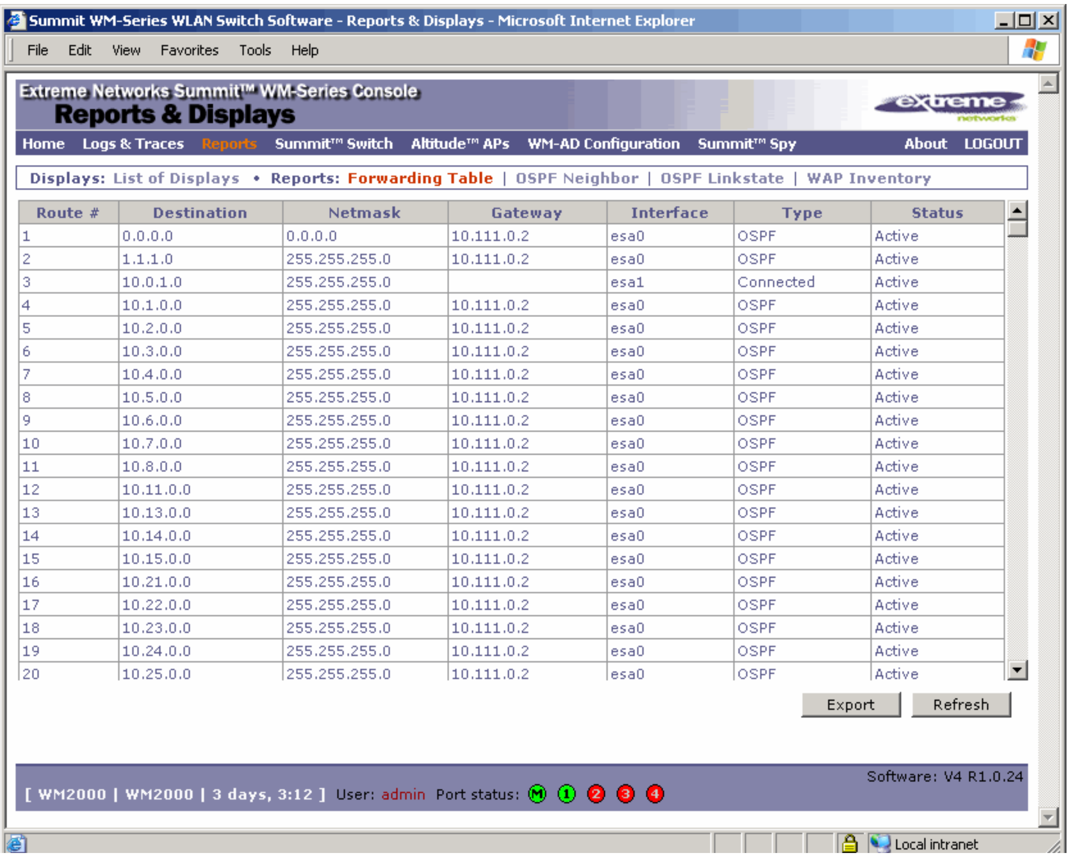
2 In the **Reports** list, click the report you want to view:

- Forwarding Table
- OSPF Neighbor
- OSPF Linkstate
- AP Inventory

NOTE

The AP Inventory report opens in a new browser window. All other reports appear in the current browser window.

The following is an example of a **Forwarding Table** report:


Summit WM-Series WLAN Switch Software - Reports & Displays - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Reports & Displays
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Displays: List of Displays • Reports: Forwarding Table | OSPF Neighbor | OSPF Linkstate | WAP Inventory
Export
Refresh
Local intranet

Route #	Destination	Netmask	Gateway	Interface	Type	Status
1	0.0.0.0	0.0.0.0	10.111.0.2	esa0	OSPF	Active
2	1.1.1.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
3	10.0.1.0	255.255.255.0		esa1	Connected	Active
4	10.1.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
5	10.2.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
6	10.3.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
7	10.4.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
8	10.5.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
9	10.6.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
10	10.7.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
11	10.8.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
12	10.11.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
13	10.13.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
14	10.14.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
15	10.15.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
16	10.21.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
17	10.22.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
18	10.23.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
19	10.24.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
20	10.25.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active

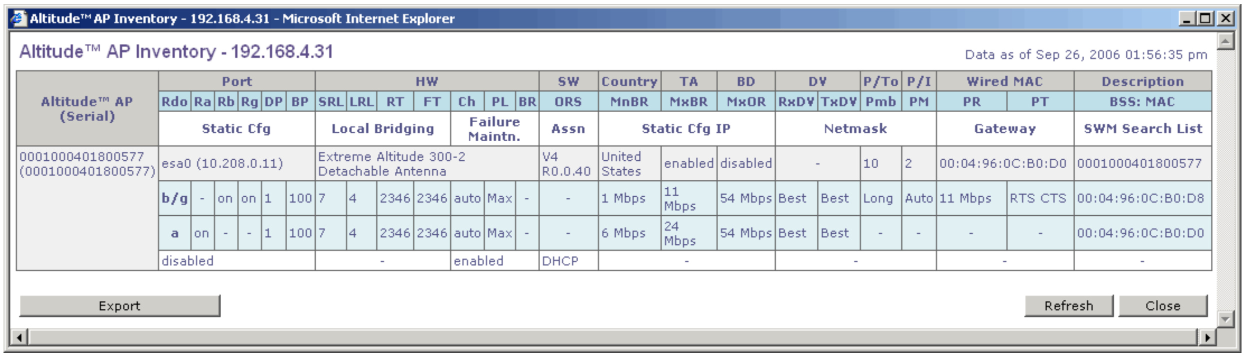
Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

NOTE

If you open only automatically refreshed reports, the Web management session timer will not be updated or reset. Your session will eventually timeout.

The following is an example of the AP Inventory report:


Altitude™ AP Inventory - 192.168.4.31 - Microsoft Internet Explorer
Export
Refresh
Close

Altitude™ AP Inventory - 192.168.4.31

Data as of Sep 26, 2006 01:56:35 pm

Altitude™ AP (Serial)	Port						HW							SW	Country	TA	BD	DV		P/To	P/I	Wired MAC		Description
	Rdo	Ra	Rb	Rg	DP	BP	SRL	LRL	RT	FT	Ch	PL	BR	ORS	MnBR	MxBR	MxOR	RxDV	TxDV	Pmb	PM	PR	PT	BSS: MAC
	Static Cfg						Local Bridging				Failure Maintn.			Assn	Static Cfg IP			Netmask				Gateway		SWM Search List
0001000401800577 (0001000401800577)	esa0 (10.208.0.11)						Extreme Altitude 300-2 Detachable Antenna							V4 R0.0.40	United States	enabled	disabled	-		10	2	00:04:96:0C:B0:D0		0001000401800577
	b/g	-	on	on	1	100	7	4	2346	2346	auto	Max	-	-	1 Mbps	11 Mbps	54 Mbps	Best	Best	Long	Auto	11 Mbps	RTS CTS	00:04:96:0C:B0:D8
	a	on	-	-	1	100	7	4	2346	2346	auto	Max	-	-	6 Mbps	24 Mbps	54 Mbps	Best	Best	-	-	-	-	00:04:96:0C:B0:D0
	disabled						-				enabled			DHCP	-			-				-		-

The following is a description of the column names and abbreviations found in the **AP Inventory** report:

- **Rdo** – Radio
- **Ra** – 802.11a radio. The data entry for an Altitude AP indicates whether the **a** radio is on or off.
- **Rb** – 802.11b protocol enabled. Possible values are **on** or **off**.
- **Rg** – 802.11g protocol enabled. Possible values are **on** or **off**.
- **DP** – DTIM period
- **BP** – Beacon Period
- **SRL** – Short Retry Limit
- **LRL** – Long Retry Limit
- **RT** – RTS Threshold
- **FT** – Fragmentation Threshold
- **Ch** – Channel served by the corresponding radio.
- **PL** – Power Level (Defined in the Altitude AP radio properties pages.)
- **BR** – Basic Rate (Only applies to Altitude APs running 3.1 or earlier.)
- **ORS** – Operational Rate Set (Only applies to Altitude APs running 3.1 or earlier.)
- **MnBR** – Minimum Basic Rate (For more information, see the Altitude AP radio configuration tabs.)
- **MxBR** – Maximum Basic Rate
- **MxOR** – Maximum Operational Rate
- **RxDV** – Receive Diversity
- **TxDV** – Tx Diversity
- **Pmb** – Preamble (long, short)
- **PM** – Protection Mode
- **PR** – Protection Rate
- **PT** – Protection Type
- **BSS** – Basic Service Set
- **MAC** – MAC address
- **BSS: MAC** – Also called BSSID, this is the MAC address of a (virtual) wireless interface on which the Altitude AP serves a BSS/WM-AD. There could be 8 per radio.

- **Port –** Ethernet Port and associated IP address of the interface on the Summit WM series switch through which the Altitude AP communicates.
- **HW** – Hardware version of the Altitude AP.
- **SW** – Software version executing on the Altitude AP.
- **TA** – Telnet access (enabled or disabled).
- **BD** – Broadcast disassociation (enabled or disabled). If enabled, whenever the Altitude AP is going offline in a controlled fashion it will send the disassociation frame to all its clients as a broadcast.
- **DV** – Diversity
- **P/To** – Poll timeout. If polling is enabled, a numeric value.
- **P/I** – Poll interval. If polling is enabled, a numeric value.
- **Wired MAC –** The physical address of the Altitude AP's wired Ethernet interface.
- **Description –** As defined on the **AP Properties** screen.
- **Failure Maintn.** – Maintain MU sessions on Altitude AP when the Altitude AP loses the connection to the Summit WM series switch.
- **Assn** – Assignment (address assignment method)
- **Static Cfg –** Altitude AP's IP address if statically configured (same as the **Static Values** radio button on the **AP Static Configuration** screen).
- **Static Cfg IP** – Statically Configured IP. If the Altitude AP's IP address is configured statically, the IP address is displayed.
- **Netmask** – If the Altitude AP's IP address is configured statically, the netmask that is statically configured for the Altitude AP.
- **Gateway** – If the Altitude AP's IP address is configured statically, the IP address of the gateway router that the Altitude AP will use.
- **HWC Search List –** The list of IP addresses that the Altitude AP is configured to try to connect to in the event that the current connection to the Summit WM series switch is lost.

To export and save a report in XML:

1 On the report screen, click **Export**. A Windows **File Download** dialog is displayed.

2 Click the **Save** button. A Windows **Save As** dialog is displayed.

NOTE

If your default XML viewer is Internet Explorer or Netscape, clicking Open will open the exported data to your display screen. You must right-click to go back to the export display. The XML data file will not be saved to your local drive.

3 Browse to the location where you want to save the exported XML data file, and in the **File name** box enter an appropriate name for the file.

4 Click **Save**. The XML data file is saved in the specified location.

10 Performing system maintenance

This chapter describes system maintenance processes, including:

- Performing Altitude AP client management
- Resetting the AP to its factory default settings
- Performing system maintenance tasks
- Performing Summit WM series switch software maintenance
- Configuring Summit WM series switch, access points, and WLAN switch software logs and traces

Performing Altitude AP client management

There are times when for service reasons or security issues, you want to cut the connection with a particular wireless device. You can view all the associated wireless devices, by MAC address, on a selected Altitude AP. You can do the following:

- Disassociate a selected wireless device from its Altitude AP.
- Add a selected wireless device's MAC address to a blacklist of wireless clients that will not be allowed to associate with the Altitude AP.
- Backup and restore the Summit WM series switch database. For more information, see "Performing Summit WM series switch software maintenance" on page 210.

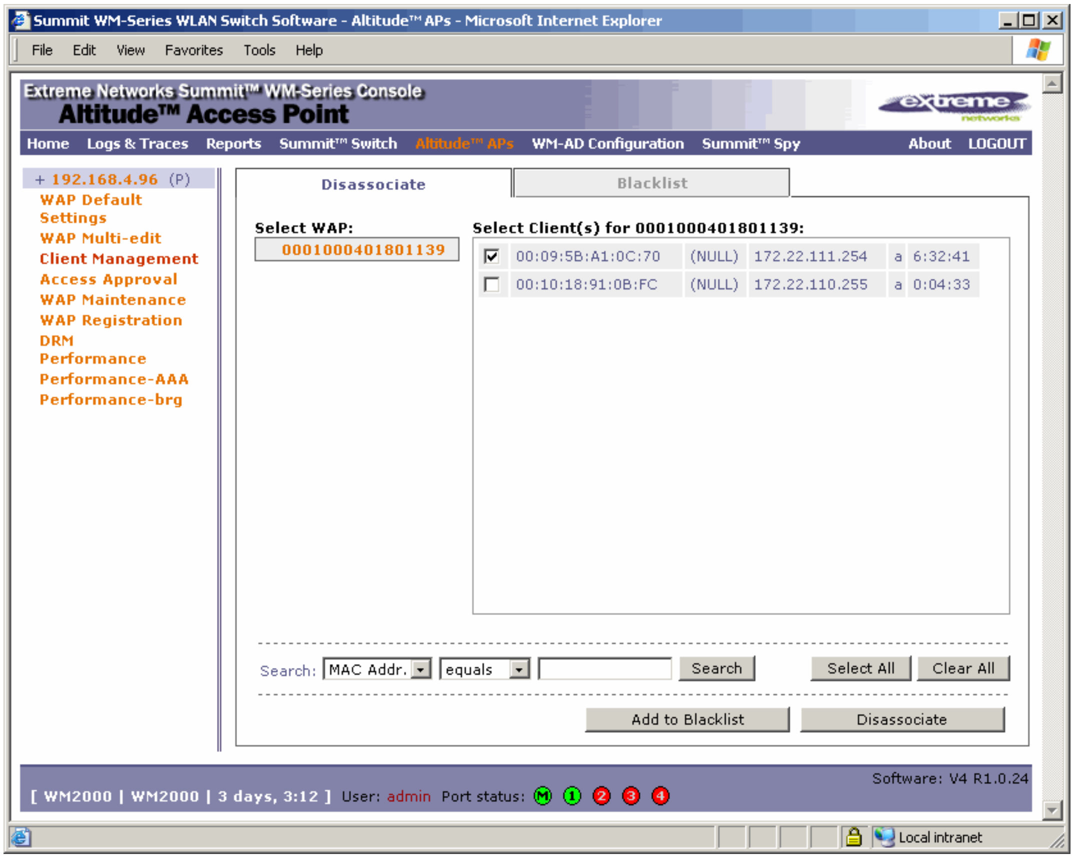
Disassociating a client

In addition to the following procedure below, you can also disassociate wireless users directly from the **Active Clients by WM-AD** screen. For more information, see Chapter 9, "Working with reports and displays."

To disassociate a wireless device client:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** screen is displayed.

2 From the left pane, click **Client Management**. The **Disassociate** tab is displayed.



Select WAP: 0001000401801139

Select Client(s) for 0001000401801139:

☑	00:09:5B:A1:0C:70	(NULL)	172.22.111.254	a	6:32:41
☐	00:10:18:91:0B:FC	(NULL)	172.22.110.255	a	0:04:33

Search: MAC Addr. equals

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

3 In the **Select AP** list, click the AP you want to disassociate.

4 In the **Select Client(s)** list, select the checkbox next to the client you want to disassociate, if applicable.

NOTE

*You can search for a client by MAC Address, IP Address or User ID, by selecting the search parameters from the drop-down lists and typing a search string in the Search box and clicking **Search**. You can also use the **Select All** or **Clear All** buttons to help you select multiple clients.*

5 Click **Disassociate**. The client's session terminates immediately.

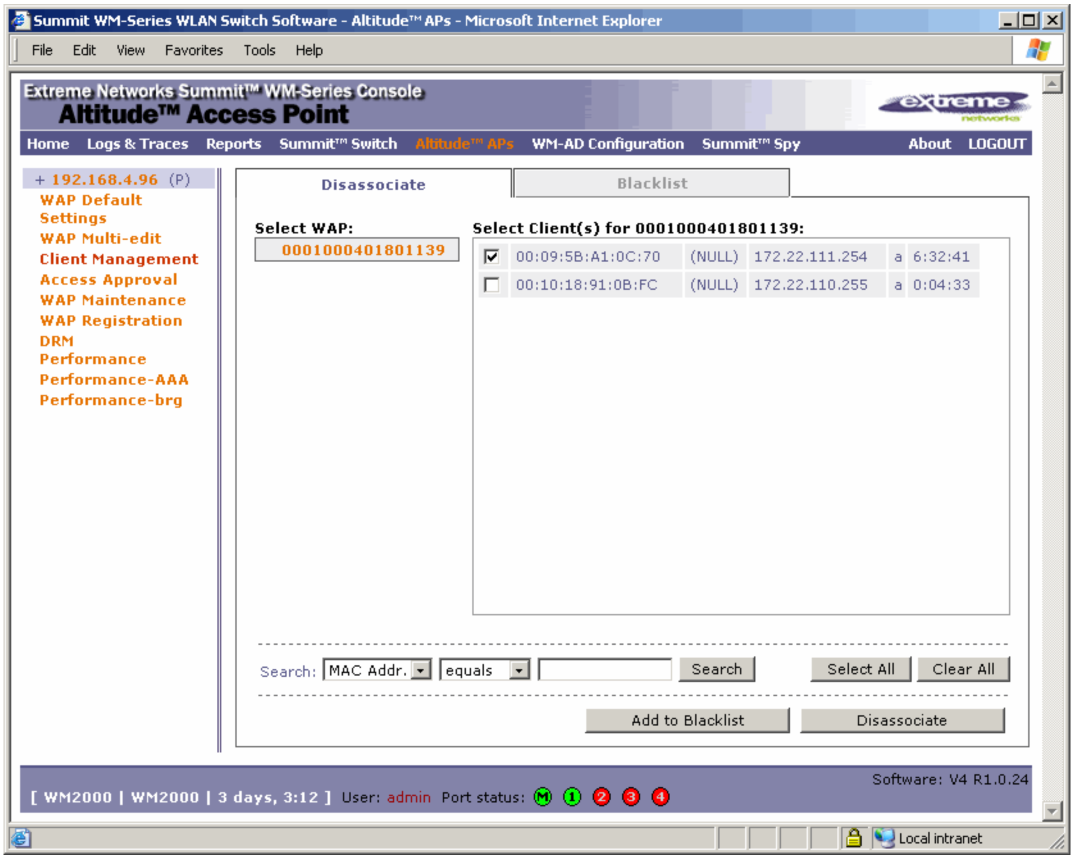
Blacklisting a client

The **Blacklist** tab displays the current list of MAC addresses that are not allowed to associate. A client is added to the blacklist by selecting it from a list of associated APs or by entering its MAC address.

To blacklist a wireless device client:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** screen is displayed.

2 From the left pane, click **Client Management**. The **Disassociate** tab is displayed.



Select WAP: 0001000401801139

Select Client(s) for 0001000401801139:

☑	00:09:5B:A1:0C:70	(NULL)	172.22.111.254	a	6:32:41
☐	00:10:18:91:0B:FC	(NULL)	172.22.110.255	a	0:04:33

Search: MAC Addr. equals

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

3 In the **Select AP** list, click the AP you want to disassociate.

4 In the **Select Client(s)** list, select the checkbox next to the client you want to disassociate, if applicable.

NOTE

You can search for a client by MAC Address, IP Address or User ID, by selecting the search parameters from the drop-down lists and typing a search string in the Search box and clicking ***Search****. You can also use the* ***Select All*** *or* ***Clear All*** *buttons to help you select multiple clients.*

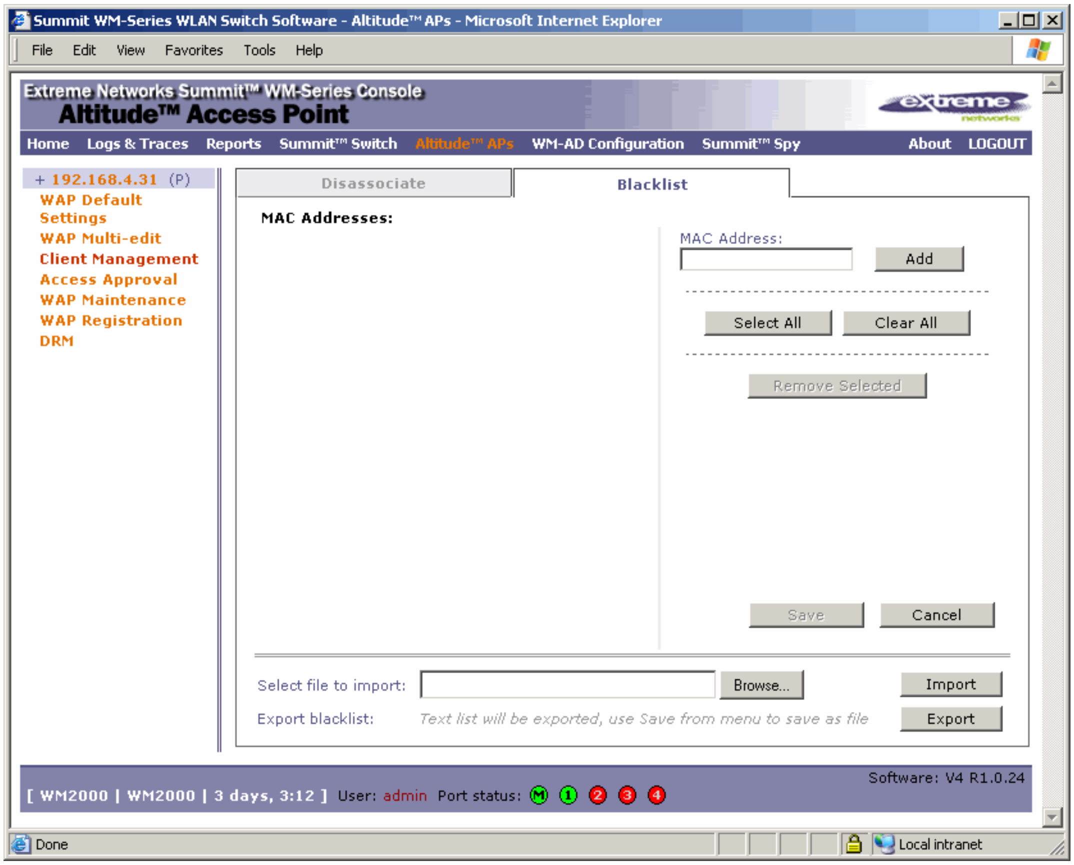
5 Click **Add to Blacklist**. The selected wireless client's MAC address is added to the blacklist.

To blacklist a wireless device client using its MAC address:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** screen is displayed.

2 From the left pane, click **Client Management**. The **Disassociate** tab is displayed.

3 Click the **Blacklist** tab.


Summit WM-Series WLAN Switch Software - Altitude™ APs - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Altitude™ Access Point
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
+ 192.168.4.31 (P)
WAP Default Settings
WAP Multi-edit
Client Management
Access Approval
WAP Maintenance
WAP Registration
DRM
Disassociate
Blacklist
MAC Addresses:
MAC Address:
Add
Select All
Clear All
Remove Selected
Save
Cancel
Select file to import:
Browse...
Import
Export blacklist:
Text list will be exported, use Save from menu to save as file
Export
Software: V4 R1.0.24
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4
Done
Local intranet

4 To add a new MAC address to the blacklist, in the **MAC Address** box enter the client's MAC address.

5 Click **Add**. The client is displayed in the **MAC Addresses** list.

NOTE

You can use the ***Select All*** *or* ***Clear All*** *buttons to help you select multiple clients.*

6 To save your changes, click **Save**.

To clear an address from the blacklist:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** screen is displayed.

2 From the left pane, click **Client Management**. The **Disassociate** tab is displayed.

3 Click the **Blacklist** tab.

4 To clear an address from the blacklist, select the corresponding checkbox in the **MAC Addresses** list.

5 Click **Remove Selected**. The selected client is removed from the list.

NOTE

You can use the ***Select All*** *or* ***Clear All*** *buttons to help you select multiple clients.*

6 To save your changes, click **Save**.

To import a list of MAC addresses for the blacklist:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** screen is displayed.

2 From the left pane, click **Client Management**. The **Disassociate** tab is displayed.

3 Click the **Blacklist** tab.

4 Click **Browse** and navigate to the file of MAC addresses you want to import and add to the blacklist.

5 Select the file, and then click **Import**. The list of MAC addresses is imported.

To export a list of MAC addresses for the blacklist:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** screen is displayed.

2 From the left pane, click **Client Management**. The **Disassociate** tab is displayed.

3 Click the **Blacklist** tab.

4 To export the current blacklist, use the browser's save option to save the file as a text (.txt) file. It is recommend that a descriptive file name is used.

5 Click **Export**. The saved blacklist file is exported.

Resetting the AP to its factory default settings

You can reset the Altitude AP to its factory default settings. The AP boot-up sequence includes a random delay interval, followed by a vulnerable time interval. During the vulnerable time interval (2 seconds), the LEDs flash in a particular sequence to indicate that the Summit WM series switch is in the vulnerable time interval. For more information, see "Understanding the Altitude AP LED status" on page 58.

If you power up the AP and interrupt the power during the vulnerable time interval three consecutive times, the next time the AP reboots, it will restore its factory defaults including the user password and the default IP settings.

WARNING!

The restoration of factory default settings does not erase the non-volatile log.

To reset the AP to its factory default settings:

1 Reboot the AP.

2 Depower and repower the AP during the vulnerable time interval.

3 Repeat Step 2 two more times.

When the AP reboots for the fourth time, after having its power supply interrupted three consecutive times, it restores its factory default settings. The AP then reboots again to put the default settings into effect.

Performing system maintenance tasks

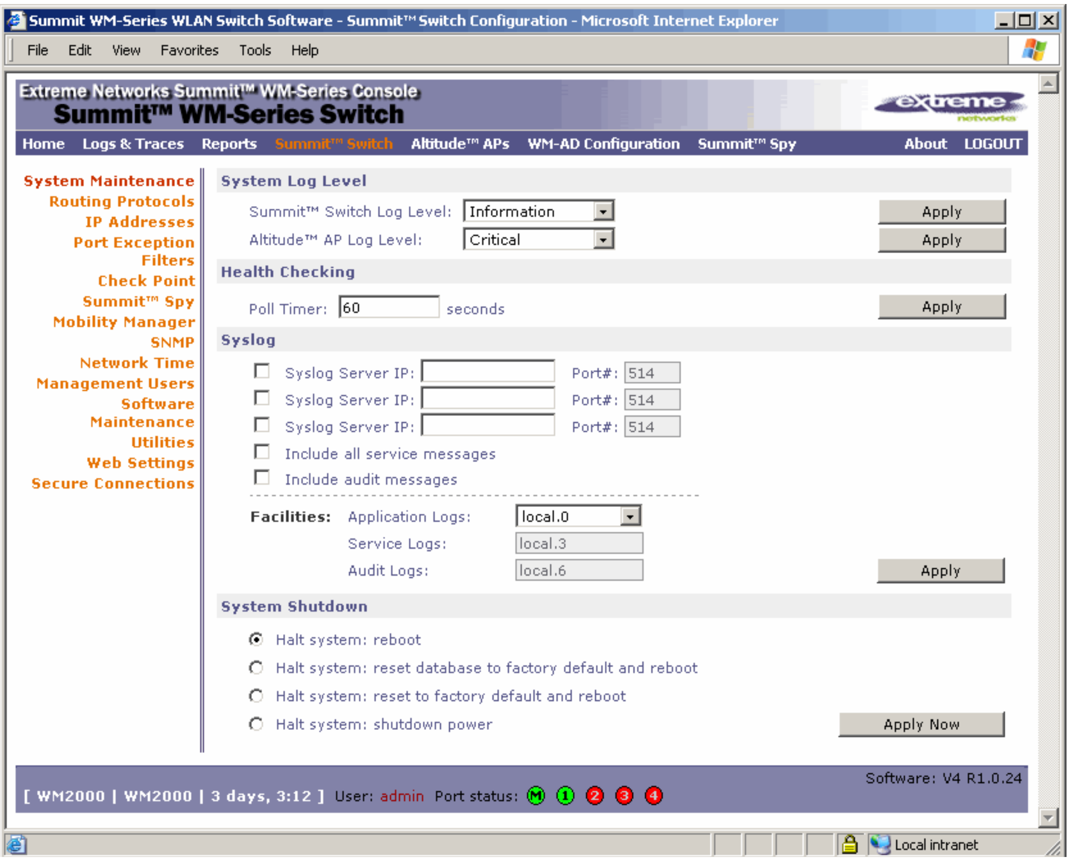
You can perform various maintenance tasks, including:

- Changing the log level
- Setting a poll interval for checking the status of the Altitude APs (Health Checking)
- Enabling and defining parameters for Syslog event reporting
- Forcing an immediate system shutdown, with or without reboot

Syslog event reporting uses the syslog protocol to relay event messages to a centralized event server on your enterprise network. In the protocol a device generates messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.

To change the log levels:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.



System Log Level

Summit™ Switch Log Level: Information

Altitude™ AP Log Level: Critical

Health Checking

Poll Timer: 60 seconds

Syslog

☐ Syslog Server IP: Port#: 514

☐ Syslog Server IP: Port#: 514

☐ Syslog Server IP: Port#: 514

☐ Include all service messages

☐ Include audit messages

Facilities: Application Logs: local.0

Service Logs: local.3

Audit Logs: local.6

System Shutdown

● Halt system: reboot

○ Halt system: reset database to factory default and reboot

○ Halt system: reset to factory default and reboot

○ Halt system: shutdown power

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

2 In the **System Log Level** section, from the **Summit Switch Log Level** drop-down list, select the least severe log level for the Controller that you want to receive: **Information**, **Minor**, **Major**, **Critical**. For example, if you select **Minor**, you receive all **Minor**, **Major** and **Critical** messages. If you select **Major** you receive all **Major** and **Critical** messages. The default is **Information**.

3 Click **Apply**.

4 From the **Altitude AP Log Level** drop-down list, select the least severe log level for the AP that you want to receive: **Information**, **Minor**, **Major**, **Critical**. The default is **Critical**.

5 Click **Apply**.

To set a poll interval:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 From the left pane, click **System Maintenance**. The **System Maintenance** screen is displayed.

3 In the **Health Checking** section, in the **Poll Timer** box, type the time interval (in seconds) for the Summit WM series switch to check that each Altitude AP is connected. The default is **60** seconds.

4 Click **Apply**.

To enable and define parameters for Syslog:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 From the left pane, click **System Maintenance**. The **System Maintenance** screen is displayed.

3 In the **Syslog** section, to enable the **Syslog** function for up to three syslog servers, select the appropriate checkboxes.

4 For each enabled syslog server, in the **IP** box, type a valid IP address for the server on the network.

5 For each enabled syslog server, in the **Port #** box, type a valid port number to connect on. The default port for syslog is **514**.

6 To include all system messages, select the **Include all service messages** checkbox. If the box is not selected, only component messages (logs and traces) are relayed. This setting applies to all three servers. The additional service messages are:

- DHCP messages reporting users receiving IP addresses
- Startup Manager Task messages reporting component startup and failure

7 To include audit messages, select the **Include audit messages** checkbox.

8 From the **Application Logs** drop-down list, select the log level (local.0 - local.6) to be sent to the syslog server. This setting applies all three servers.

9 If the **Include all service messages** checkbox is selected, the **Service Logs** drop-down list becomes selectable. Select the log level (local.0 - local.6) to be sent to the syslog server. This setting applies all three servers.

10 If you selected the **Include audit messages** checkbox, the **Audit Logs** drop-down list becomes available. Select the log level (local.0 - local.6) to be sent to the syslog server. This setting applies all three servers.

11 To apply your changes, click on the **Apply** button.

NOTE

The syslog daemon must be running on both the Summit WM series switch and on the remote syslog server before the logs can be synchronized. If you change the log level on the Summit WM series switch, you must also modify the appropriate setting in the syslog configuration on remote syslog server.

Table 17 shows Syslog and Summit WM series switch, access points, and WLAN switch software event log mapping.

Table 17: Syslog and Summit WM series switch, access points, and WLAN switch software event log mapping

Syslog Event	Summit WM series switch, access points, and WLAN switch software Event
LOG_CRIT	Critical
LOG_ERR	Major
LOG_WARNING	Minor
LOG_INFO	Information
LOG_DEBUG	Trace

To force an immediate system shutdown:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 From the left pane, click **System Maintenance**. The **System Maintenance** screen is displayed.

3 To shut down the system, including associated Altitude APs, select the appropriate shut down option:

- Halt system: reboot
- Halt system: reset database to factory default and reboot – Restores all aspects of the system configuration to the initial settings. However, the Management IP address and license key are preserved. This permits the user to remain connected through the Management interface.
- Halt system: reset to factory default and reboot – Resets the entire system configuration to the factory shipping state. The Management IP address reverts to 192.168.10.1 and the license key is removed.
- Halt system – The system enters the halted state, which stops all functional services and the application. To restart the system, the power to the system must be reset.

4 Click **Apply Now**. The system is immediately halted.

Performing Summit WM series switch software maintenance

You can update the core Summit WM series switch software files, and the Operating System (OS) software using the Software Maintenance function. A facility to backup and restore the Summit WM series switch database is also available. The maintenance interface also includes the product key maintenance, for first-time setup and upgrades, if appropriate. For more information, see "Applying the product license key" on page 41.

WARNING!

During a system upgrade from v3.1 to v4 R0.x.x, it is recommended that you install your new v4 license key BEFORE upgrading the software if you have manually configured radio channels.

If your Summit WM series switch has a v3.1 license key when it is upgraded, the key will be rejected and the Summit WM series switch will revert to a factory default DEMO region setting. Whenever the licensed region changes on the Summit WM series switch, all Altitude APs are changed to ***Auto Channel Select*** *to prevent possible infractions to local RF regulatory requirements. If this occurs, all manually configured radio channel settings will be lost.*

Installing the new license key before upgrading will prevent the Summit WM series switch from changing the licensed region, and in addition, manually configured channel settings will be maintained.

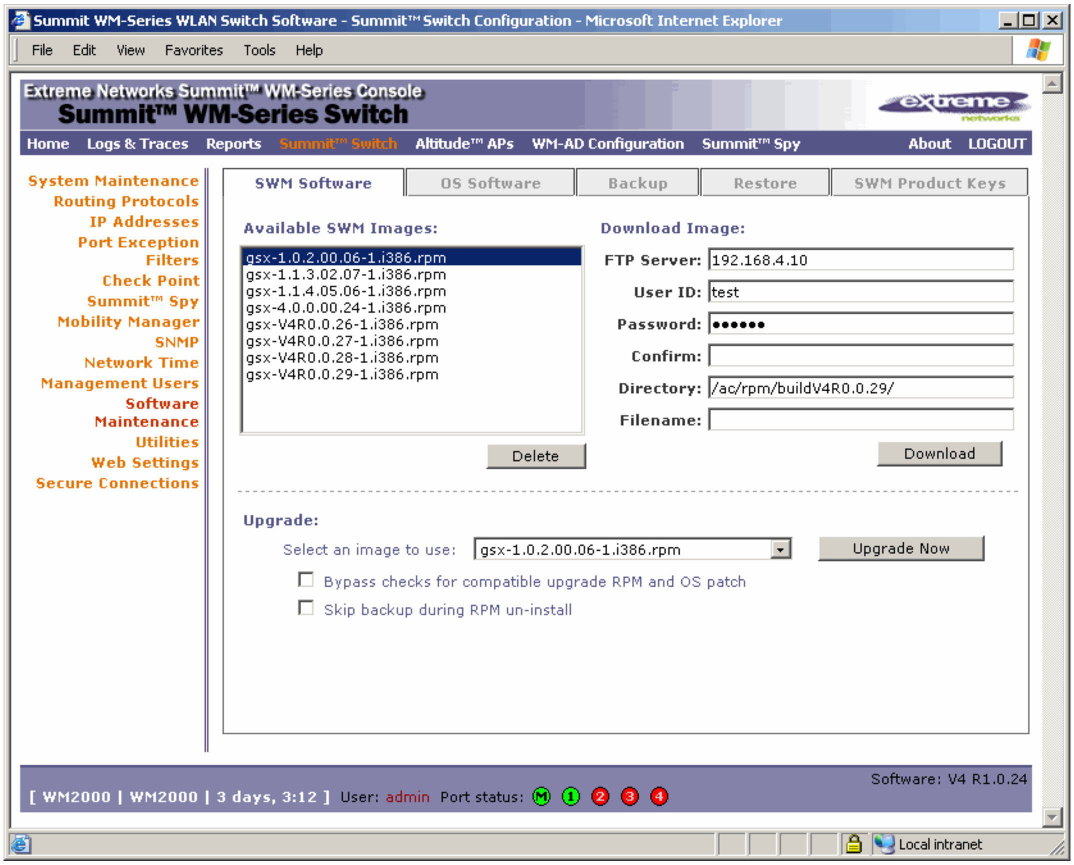
Updating Summit WM series switch software

You can update the core Summit WM series switch software files using the Software Maintenance function.

To upgrade Summit WM series switch software:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.



Available SWM Images:

gsx-1.0.2.00.06-1.i386.rpm
gsx-1.1.3.02.07-1.i386.rpm
gsx-1.1.4.05.06-1.i386.rpm
gsx-4.0.0.00.24-1.i386.rpm
gsx-V4R0.0.26-1.i386.rpm
gsx-V4R0.0.27-1.i386.rpm
gsx-V4R0.0.28-1.i386.rpm
gsx-V4R0.0.29-1.i386.rpm

Download Image:

FTP Server: 192.168.4.10
User ID: test
Password: ●●●●●●
Confirm:
Directory: /ac/rpm/buildV4R0.0.29/
Filename:

Upgrade:

Select an image to use: gsx-1.0.2.00.06-1.i386.rpm

□ Bypass checks for compatible upgrade RPM and OS patch
□ Skip backup during RPM un-install

Software: V4 R1.0.24
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

The **Available SWM Images** section displays the list of software versions that have been downloaded and are available.

3 In the **Upgrade** section, select an image from the **Select an image to use** drop-down list.

NOTE

It is recommended that the Bypass checks for compatible upgrade RPM and OS patch and the Skip backup during RPM un-install options remain disabled.

4 To launch the upgrade with the selected image, click on the **Upgrade Now** button.

5 In the dialog box that is displayed, confirm the upgrade.

At this point, all sessions are closed. The previous software is uninstalled automatically. The new software is installed. The Summit WM series switch reboots automatically. The database is updated and migrated.

To download a new Summit WM series switch software image:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.

3 To download a new image to be added to the list, in the **Download Image** section type the following:

- **FTP Server** – The IP of the FTP server to retrieve the image file from.
- **User ID** – The user ID that the controller should use when it attempts to log in to the FTP server.
- **Password** – The corresponding password for the user ID.
- **Confirm** – The corresponding password for the user ID to confirm it was typed correctly.
- **Directory** – The directory on the server in which the image file that is to be retrieved is stored.
- **Filename** – The name of the image file to retrieve.
- **Platform** – The AP hardware type to which the image applies. The are several types of AP and they require different images.

4 Click **Download**. The image is downloaded and added to the list.

To delete a Summit WM series switch software image:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.

3 To delete a software image from the list, in the **Available SWM Images** list, click the image.

4 Click **Delete**. The image is removed from the list.

Updating operating system software

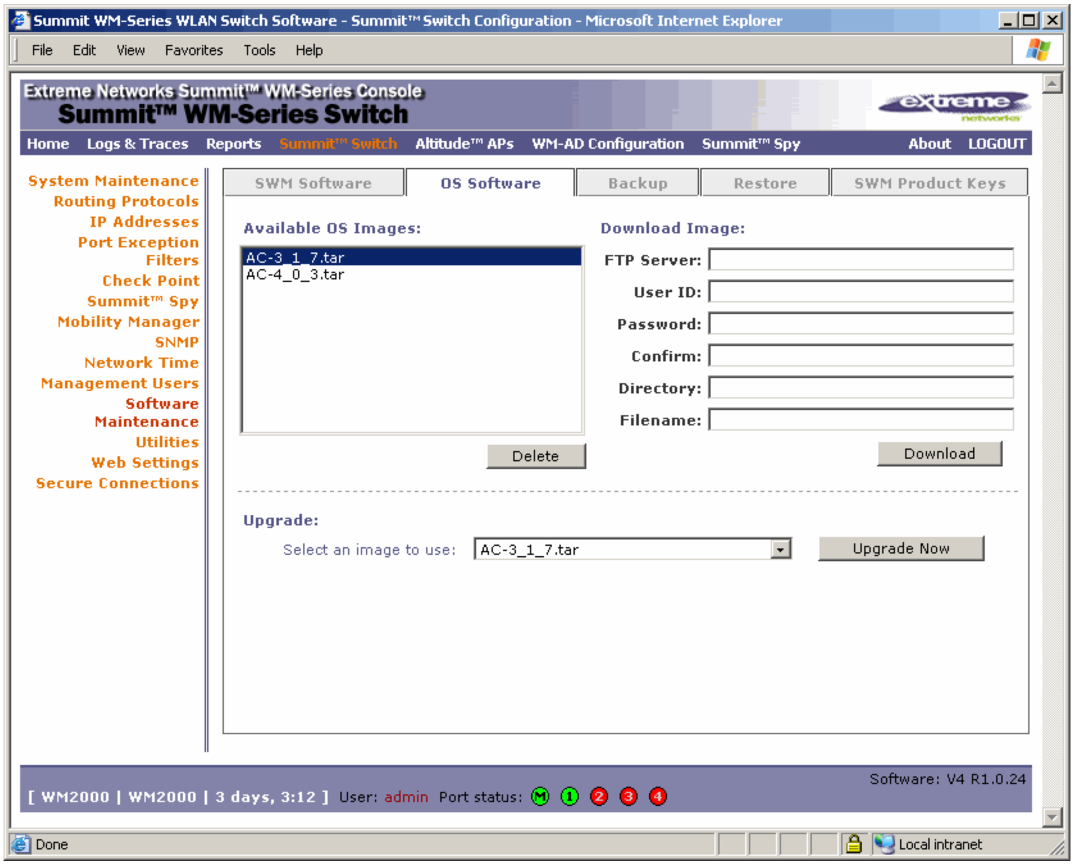
You can update the Operating System (OS) software using the Software Maintenance function.

To upgrade operating system software:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.

3 Click the **OS Software** tab.



Available OS Images:
AC-3_1_7.tar
AC-4_0_3.tar

Download Image:
FTP Server:
User ID:
Password:
Confirm:
Directory:
Filename:

Upgrade:
Select an image to use: AC-3_1_7.tar

Software: V4 R1.0.24
[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

The **Available OS Images** section displays the list of software versions that have been downloaded and are available.

4 In the **Upgrade** section, select an image from the **Select an image to use** drop-down list.

5 To launch the upgrade with the selected image, click **Upgrade Now**.

6 In the dialog box that is displayed, confirm the upgrade.

At this point, all sessions are closed. The previous software is uninstalled automatically. The new software is installed. The Summit WM series switch reboots automatically.

To download a new operating system software image:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.

3 Click the **OS Software** tab.

4 To download a new image to be added to the list, in the **Download Image** section type the following:

- **FTP Server** – The IP of the FTP server to retrieve the image file from.
- **User ID** – The user ID that the controller should use when it attempts to log in to the FTP server.
- **Password** – The corresponding password for the user ID.
- **Confirm** – The corresponding password for the user ID to confirm it was typed correctly.
- **Directory** – The directory on the server in which the image file that is to be retrieved is stored.
- **Filename** – The name of the image file to retrieve.
- **Platform** – The AP hardware type to which the image applies. The are several types of AP and they require different images.

5 Click **Download**. The image is downloaded and added to the list.

To delete a Summit WM series switch software image:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.

3 Click the **OS Software** tab.

4 To delete a software image from the list, in the **Available OS Images** list, click the image.

5 Click **Delete**. The image is removed from the list.

Backing up Summit WM series switch software

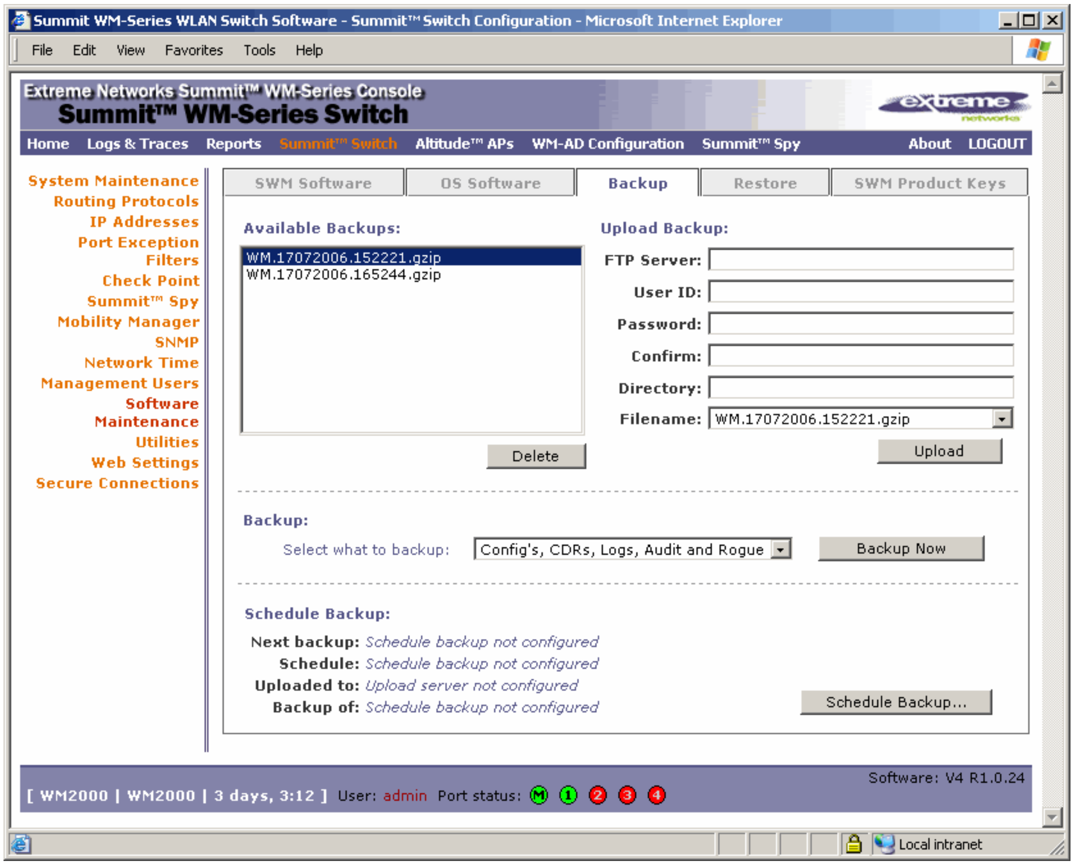
You can backup the Summit WM series switch database. You can also schedule the backups to occur. When a scheduled backup is defined, you can configure to have the scheduled backup copied to an FTP server when the backup is complete.

To back up the Summit WM series switch software:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.

3 Click the **Backup** tab.



Available Backups:
WM.17072006.152221.gzip
WM.17072006.165244.gzip

Filename: WM.17072006.152221.gzip

Select what to backup: Config's, CDRs, Logs, Audit and Rogue

Next backup: *Schedule backup not configured*
Schedule: *Schedule backup not configured*
Uploaded to: *Upload server not configured*
Backup of: *Schedule backup not configured*

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4
Software: V4 R1.0.24

The **Available Backups** section displays the list items that have been backed up and are available.

4 In the **Backup** section, select an item from the **Select what to backup** drop-down list.

5 To launch the backup with the selected items, click on the **Backup Now** button.

6 In the dialog box that is displayed, confirm the backup. The items are backed up.

To upload a new backup:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.

3 Click the **Backup** tab.

4 To upload a new backup, which will be added to the list, in the **Upload Backup** section type the following:

- **FTP Server** – The IP of the FTP server to retrieve the image file from.
- **User ID** – The user ID that the controller should use when it attempts to log in to the FTP server.
- **Password** – The corresponding password for the user ID.
- **Confirm** – The corresponding password for the user ID to confirm it was typed correctly.
- **Directory** – The directory on the server where the image file will be stored.
- **Filename** – The name that will be given to the image file when it is stored on the FTP server.

- **Platform –** The AP hardware type to which the image applies. The are several types of AP and they require different images.

5 Click **Upload**. The backup is uploaded and added to the list.

To delete a backup:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.

3 Click the **Backup** tab.

4 To delete a backup from the list, in the **Available Backups** list, click the backup.

5 Click **Delete**. The backup is removed from the list.

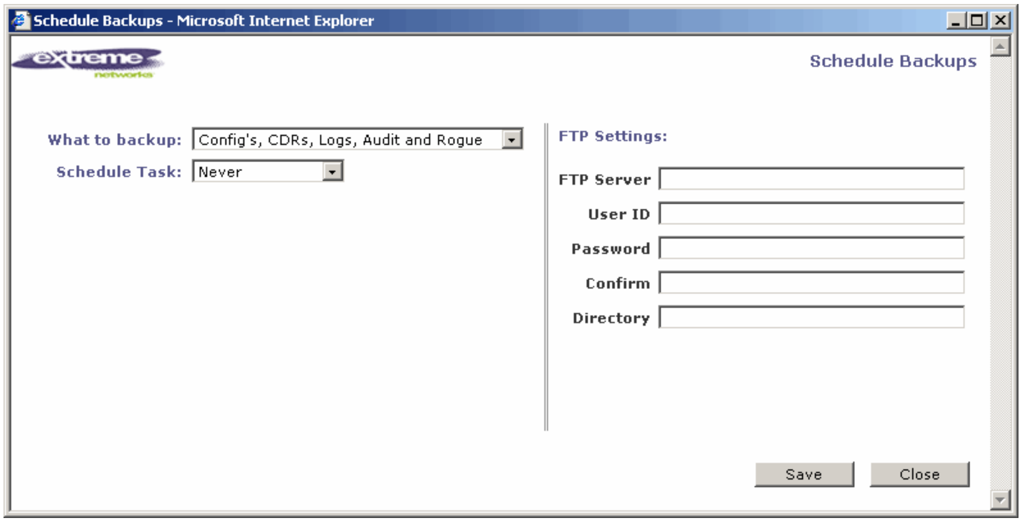
To schedule a backup:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.

3 Click the **Backup** tab.

4 Click **Schedule Backup**. The **Schedule Backups** screen is displayed.



What to backup: Config's, CDRs, Logs, Audit and Rogue

Schedule Task: Never

FTP Settings:

FTP Server

User ID

Password

Confirm

Directory

5 In the **What to backup** drop-down list, select what you want to backup:

- Config's, CDRs, Logs, Audit and Rogue
- Configurations only
- CDRs only
- Logs only
- Audit only
- Rogue only

6 In the **Schedule task** drop-down list, select the frequency of the backup:

- Daily
- Weekly
- Monthly
- Never

7 In the **FTP settings** section, type the following:

- **FTP Server –** The IP of the FTP server to where the scheduled backup will be copied to.
- **User ID –** The user ID that the controller should use when it attempts to log in to the FTP server.
- **Password –** The corresponding password for the user ID
- **Confirm –** The corresponding password for the user ID to confirm it was typed correctly.
- **Directory –** The directory on the server where the image file will be stored.

8 To save your changes, click **Save**.

Restoring Summit WM series switch software

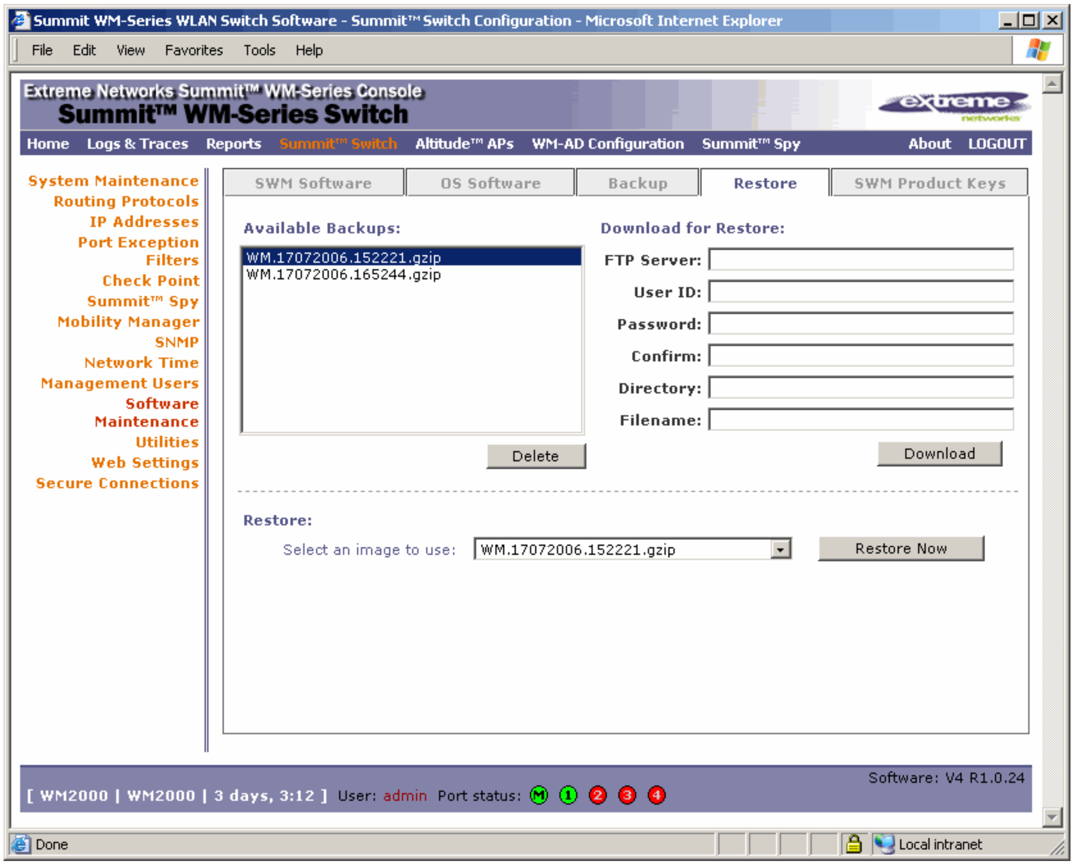
You can restore the Summit WM series switch database.

To restore the Summit WM series switch software:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.

3 Click the **Restore** tab.



Available Backups:

WM.17072006.152221.gzip
WM.17072006.165244.gzip

Download for Restore:

FTP Server:
User ID:
Password:
Confirm:
Directory:
Filename:

Restore:

Select an image to use: WM.17072006.152221.gzip

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

The **Available Backups** section displays the list items that have been backed up and are available.

4 In the **Restore** section, select an item from the **Select an image to use** drop-down list.

5 To launch the backup with the selected items, click on the **Restore Now** button.

6 In the dialog box that is displayed, confirm the restore. The image is restored.

To download for restore:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 From the left pane, click **Software Maintenance**. The **System Maintenance** screen is displayed.

3 Click the **Restore** tab.

4 To download an image for restore, which will be added to the list, in the **Download for Restore** section type the following:

- **FTP Server** –The FTP server to retrieve the image file from.
- **User ID** – The user ID that the controller should use when it attempts to log in to the FTP server.
- **Password** – The corresponding password for the user ID.
- **Confirm** – The corresponding password for the user ID to confirm it was typed correctly.
- **Directory** – The directory on the server in which the image file that is to be retrieved is stored.
- **Filename** – The name of the image file to retrieve.

- **Platform** – The AP hardware type to which the image applies. The are several types of AP and they require different images.

5 Click **Download**. The image is downloaded and added to the list.

To delete a backup available for restore:

1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

2 From the left pane, click **Software Maintenance**. The **System Maintenance** screen is displayed.

3 Click the **Restore** tab.

4 To delete a backup from the list, in the **Available Backups** list, click the backup.

5 Click **Delete**. The backup is removed from the list.

Upgrading a Summit WM series switch using SFTP

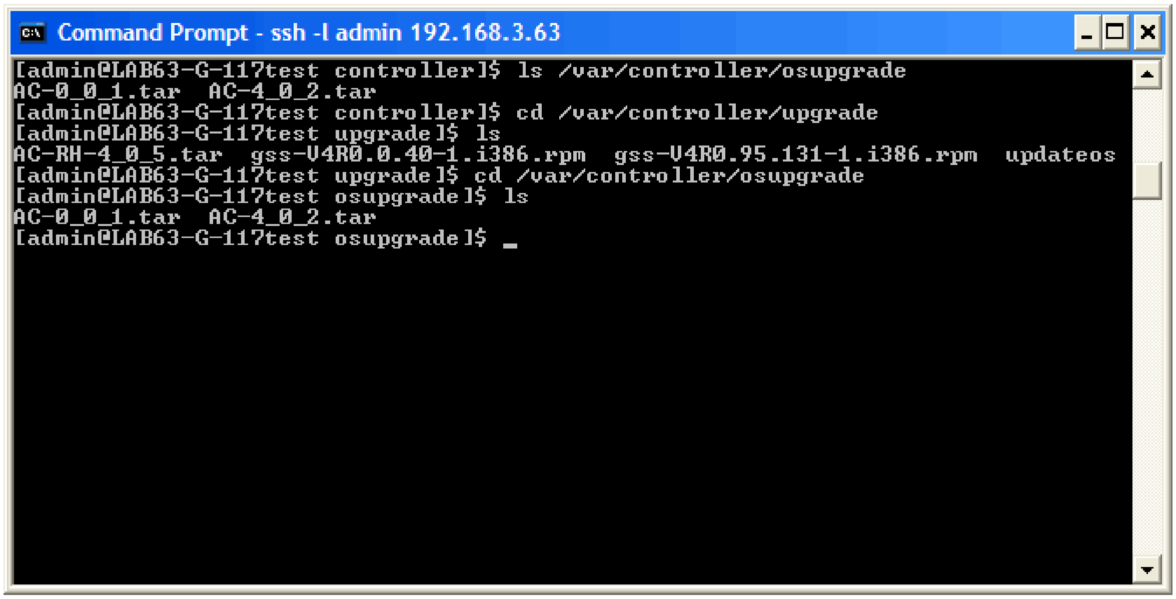
You can upload an image file to the Summit WM series switch using Secure FTP (SFTP). The Summit WM series switch supports any SFTP client.

NOTE

You must enable management traffic before you try to connect with a SFTP client. Specify the exact image path for the corresponding SW package (see directory information below). Otherwise, the Summit WM series switch cannot locate them for SW upgrades/updates.

To upload an image file:

1 Launch the SFTP client, point it to the Summit WM series switch and login in. The exact details of how to do this will depend on the client used. The following uses putty as an example:



```
[admin@LAB63-G-117test controller]$ ls /var/controller/osupgrade
AC-0_0_1.tar  AC-4_0_2.tar
[admin@LAB63-G-117test controller]$ cd /var/controller/upgrade
[admin@LAB63-G-117test upgrade]$ ls
AC-RH-4_0_5.tar  gss-V4R0.0.40-1.i386.rpm  gss-V4R0.95.131-1.i386.rpm  updateos
[admin@LAB63-G-117test upgrade]$ cd /var/controller/osupgrade
[admin@LAB63-G-117test osupgrade]$ ls
AC-0_0_1.tar  AC-4_0_2.tar
[admin@LAB63-G-117test osupgrade]$ _
```

2 Change to the directory to receive the uploaded file:
   - For AP images change to: /var/tftp/chantry
   - For Summit WM series switch images change to: /var/controller/upgrade
   - For OS archives change to: /var/controller/osupgrade

3 Upload the image file using the SFTP client upload feature.

4 To complete a Summit WM series switch upgrade or an AP upgrade go to the appropriate **Software Maintenance** screen. For more information, see "Updating Summit WM series switch software" on page 211 or "Updating operating system software" on page 212.

Configuring Summit WM series switch, access points, and WLAN switch software logs and traces

The system stores configuration data and log files. These files include:

- event and alarm logs (triggered by events)
- trace logs (triggered by component activity)
- accounting files (created every 30 minutes, to a maximum of six files)

The files are stored in the operating system and have a maximum size of one GB. The accounting files are stored in flat files in a directory that is created every day. Eight directories are maintained in a circular buffer (when all are full, the most recent replaces the earliest).

Viewing log, alarm and trace messages

The Summit WM series switch generates three types of messages:

- Logs (including alarms) – Messages that are triggered by events
- Audits – Files that record administrative changes made to the system (the GUI Audit displays changes to the Graphical User Interface on the Summit WM series switch)
- Traces – Messages that display activity by component, for system debugging, troubleshooting and internal monitoring of software

NOTE

In order for the Debug Info option on the Altitude AP Traces screen to return Trace messages, this option must enabled while Altitude AP debug commands are running. To do so, you need to run an Altitude AP CLI command to turn on a specific Altitude AP debug. Once the CLI command is run, select the Debug Info option, and then click Retrieve Traces. For more information, see the Summit WM series switch, access points, and WLAN switch software CLI Reference Guide.

Because Altitude AP debugging can affect the normal operation of Altitude AP service, enabling debugging is not recommended, unless specific instructions are provided.

Logs including alarms

The log messages contain the time of event, severity, source component and any details generated by the source component. The messages are classified at four levels of severity:

- Informational, the activity of normal operation
- Minor (alarm)
- Major (alarm)
- Critical (alarm)

The alarm messages (minor, major or critical log messages) are triggered by activities that meet certain conditions that should be known and dealt with.

Examples of events on the Summit WM series switch that generate an alarm message:

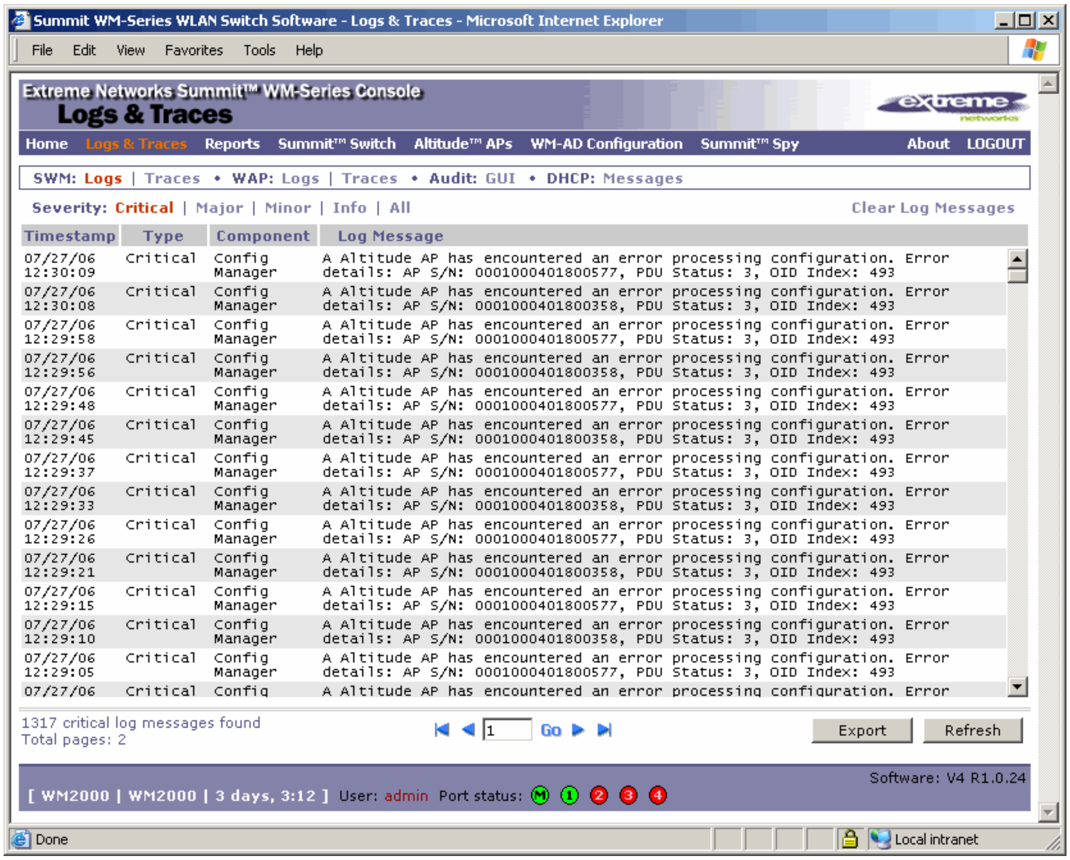
- Reboot due to failure
- Software upgrade failure on the Summit WM series switch
- Software upgrade failure on the Altitude AP
- Detection of rogue access point activity without valid ID

If SNMP is enabled on the Summit WM series switch, alarm conditions will trigger a trap in SNMP (Simple Network Management Protocol). An SNMP trap is an event notification sent by the managed agent (a network device) to the management system to identify the occurrence of conditions.

To view logs:

1 From the main menu, click **Logs & Traces**. The **Logs & Traces** screen is displayed.

2 Click one of the **Log** tabs. The following is an example of the Summit WM series switch logs:



Summit WM-Series WLAN Switch Software - Logs & Traces - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Logs & Traces
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
SWM: Logs | Traces • WAP: Logs | Traces • Audit: GUI • DHCP: Messages
Severity: Critical | Major | Minor | Info | All
Clear Log Messages

Timestamp	Type	Component	Log Message
07/27/06 12:30:09	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:30:08	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:29:58	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:29:56	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:29:48	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:29:45	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:29:37	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:29:33	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:29:26	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:29:21	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:29:15	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:29:10	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:29:05	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06	Critical	Config	A Altitude AP has encountered an error processing configuration. Error

1317 critical log messages found
Total pages: 2

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

The events are displayed in chronological order, sorted by the **Timestamp** column.

3 To sort the display by **Type** or **Component**, click the appropriate column heading.

4 To filter the logs by severity, in order to display only **Info**, **Minor**, **Major**, or **Critical** logs, click the appropriate **Log** tab at the top of the screen.

5 To refresh the information in any display, click **Refresh**.

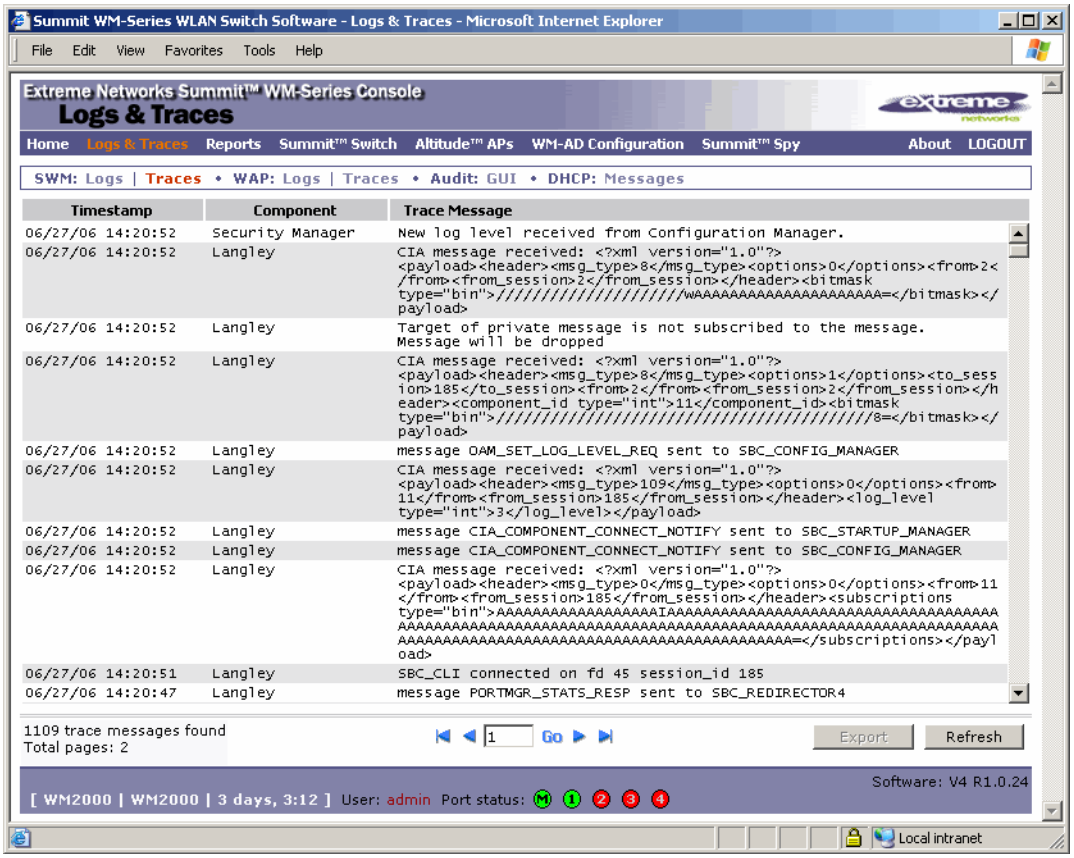
6 To export information from a display as an HTML file, click the **Export** button.

The component called "Langley" is the term for the inter-process messaging infrastructure on the Summit WM series switch.

To view traces:

1 From the main menu, click **Logs & Traces**. The **Logs & Traces** screen is displayed.

2 Click one of the **Traces** tabs. The following is an example of the Summit WM series switch traces:


Summit WM-Series WLAN Switch Software - Logs & Traces - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Logs & Traces
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
SWM: Logs | Traces • WAP: Logs | Traces • Audit: GUI • DHCP: Messages
Go
Export
Refresh
M 1 2 3 4
Local intranet

Timestamp	Component	Trace Message
06/27/06 14:20:52	Security Manager	New log level received from Configuration Manager.
06/27/06 14:20:52	Langley	CIA message received: <?xml version="1.0"?><payload><header><msg_type>8</msg_type><options>0</options><from>2</from><from_session>2</from_session></header><bitmask type="bin">/////////////////////wAAAAAAAAAAAAAAAAAAAAA=</bitmask></payload>
06/27/06 14:20:52	Langley	Target of private message is not subscribed to the message. Message will be dropped
06/27/06 14:20:52	Langley	CIA message received: <?xml version="1.0"?><payload><header><msg_type>8</msg_type><options>1</options><to_session>185</to_session><from>2</from><from_session>2</from_session></header><component_id type="int">11</component_id><bitmask type="bin">//8=</bitmask></payload>
06/27/06 14:20:52	Langley	message OAM_SET_LOG_LEVEL_REQ sent to SBC_CONFIG_MANAGER
06/27/06 14:20:52	Langley	CIA message received: <?xml version="1.0"?><payload><header><msg_type>109</msg_type><options>0</options><from>11</from><from_session>185</from_session></header><log_level type="int">3</log_level></payload>
06/27/06 14:20:52	Langley	message CIA_COMPONENT_CONNECT_NOTIFY sent to SBC_STARTUP_MANAGER
06/27/06 14:20:52	Langley	message CIA_COMPONENT_CONNECT_NOTIFY sent to SBC_CONFIG_MANAGER
06/27/06 14:20:52	Langley	CIA message received: <?xml version="1.0"?><payload><header><msg_type>0</msg_type><options>0</options><from>11</from><from_session>185</from_session></header><subscriptions type="bin">AAAAAAAAAAAAAAAAAAIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=</subscriptions></payload>
06/27/06 14:20:51	Langley	SBC_CLI connected on fd 45 session_id 185
06/27/06 14:20:47	Langley	message PORTMGR_STATS_RESP sent to SBC_REDIRECTOR4

1109 trace messages found
Total pages: 2

1

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status:

The events are displayed in chronological order, sorted by the **Timestamp** column.

3 To sort the display by **Type** or **Component**, click the appropriate column heading.

4 To filter the traces by severity, in order to display only **Info**, **Minor**, **Major**, or **Critical** traces, click the appropriate **Traces** tab at the top of the screen.

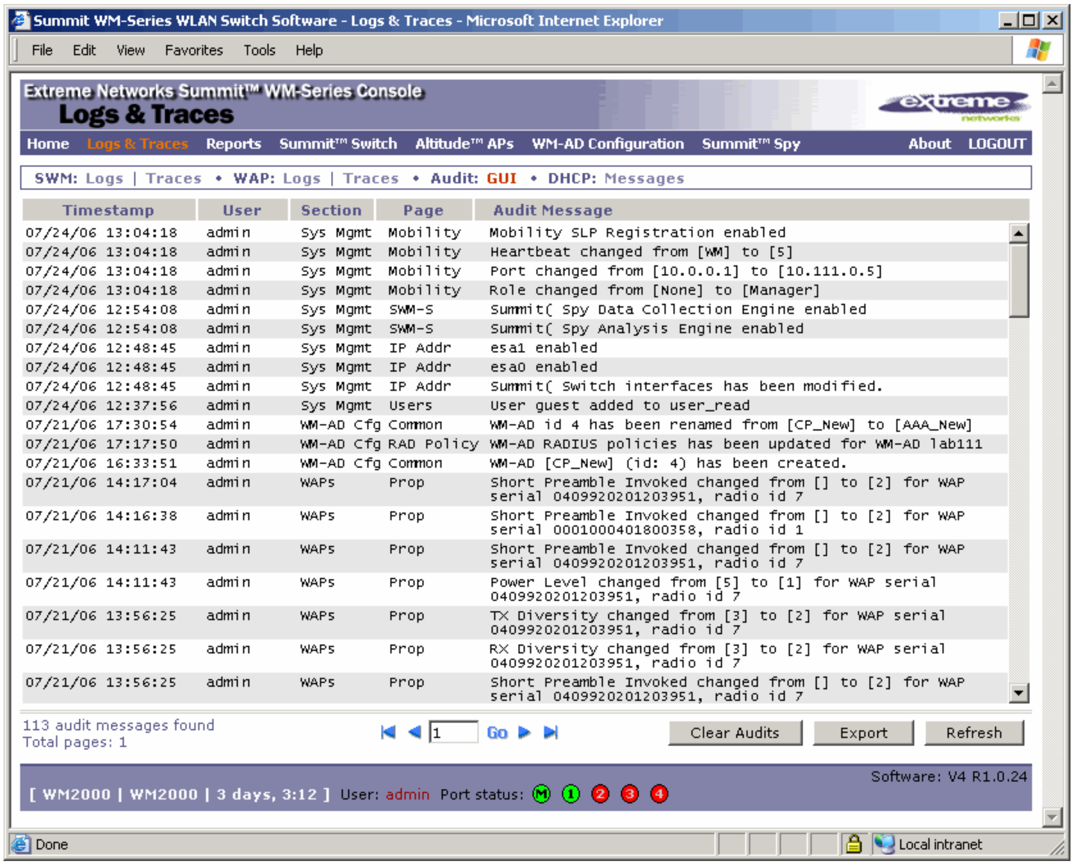
5 To refresh the information in any display, click **Refresh**.

6 To export information from a display as an HTML file, click the **Export** button.

To view audits:

1 From the main menu, click **Logs & Traces**. The **Logs & Traces** screen is displayed.

2 Click the **Audit: GUI** tab. The **Audit** screen is displayed.


Summit WM-Series WLAN Switch Software - Logs & Traces - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Logs & Traces
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
SWM: Logs | Traces • WAP: Logs | Traces • Audit: GUI • DHCP: Messages
Clear Audits
Export
Refresh
Go
Done
Local intranet

Timestamp	User	Section	Page	Audit Message
07/24/06 13:04:18	admin	Sys Mgmt	Mobility	Mobility SLP Registration enabled
07/24/06 13:04:18	admin	Sys Mgmt	Mobility	Heartbeat changed from [WM] to [5]
07/24/06 13:04:18	admin	Sys Mgmt	Mobility	Port changed from [10.0.0.1] to [10.111.0.5]
07/24/06 13:04:18	admin	Sys Mgmt	Mobility	Role changed from [None] to [Manager]
07/24/06 12:54:08	admin	Sys Mgmt	SWM-S	Summit(Spy Data Collection Engine enabled
07/24/06 12:54:08	admin	Sys Mgmt	SWM-S	Summit(Spy Analysis Engine enabled
07/24/06 12:48:45	admin	Sys Mgmt	IP Addr	esa1 enabled
07/24/06 12:48:45	admin	Sys Mgmt	IP Addr	esa0 enabled
07/24/06 12:48:45	admin	Sys Mgmt	IP Addr	Summit(Switch interfaces has been modified.
07/24/06 12:37:56	admin	Sys Mgmt	Users	User guest added to user_read
07/21/06 17:30:54	admin	WM-AD Cfg	Common	WM-AD id 4 has been renamed from [CP_New] to [AAA_New]
07/21/06 17:17:50	admin	WM-AD Cfg	RAD Policy	WM-AD RADIUS policies has been updated for WM-AD lab111
07/21/06 16:33:51	admin	WM-AD Cfg	Common	WM-AD [CP_New] (id: 4) has been created.
07/21/06 14:17:04	admin	WAPs	Prop	Short Preamble Invoked changed from [] to [2] for WAP serial 0409920201203951, radio id 7
07/21/06 14:16:38	admin	WAPs	Prop	Short Preamble Invoked changed from [] to [2] for WAP serial 0001000401800358, radio id 1
07/21/06 14:11:43	admin	WAPs	Prop	Short Preamble Invoked changed from [] to [2] for WAP serial 0409920201203951, radio id 7
07/21/06 14:11:43	admin	WAPs	Prop	Power Level changed from [5] to [1] for WAP serial 0409920201203951, radio id 7
07/21/06 13:56:25	admin	WAPs	Prop	TX Diversity changed from [3] to [2] for WAP serial 0409920201203951, radio id 7
07/21/06 13:56:25	admin	WAPs	Prop	RX Diversity changed from [3] to [2] for WAP serial 0409920201203951, radio id 7
07/21/06 13:56:25	admin	WAPs	Prop	Short Preamble Invoked changed from [] to [2] for WAP serial 0409920201203951, radio id 7

113 audit messages found
Total pages: 1

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status: M 1 2 3 4

The events are displayed in chronological order, sorted by the **Timestamp** column.

3 To sort the display by **User**, **Section**, **Page**, or **Audit Message**, click the appropriate column heading.

4 To clear the audits from the list, click **Clear Audits**.

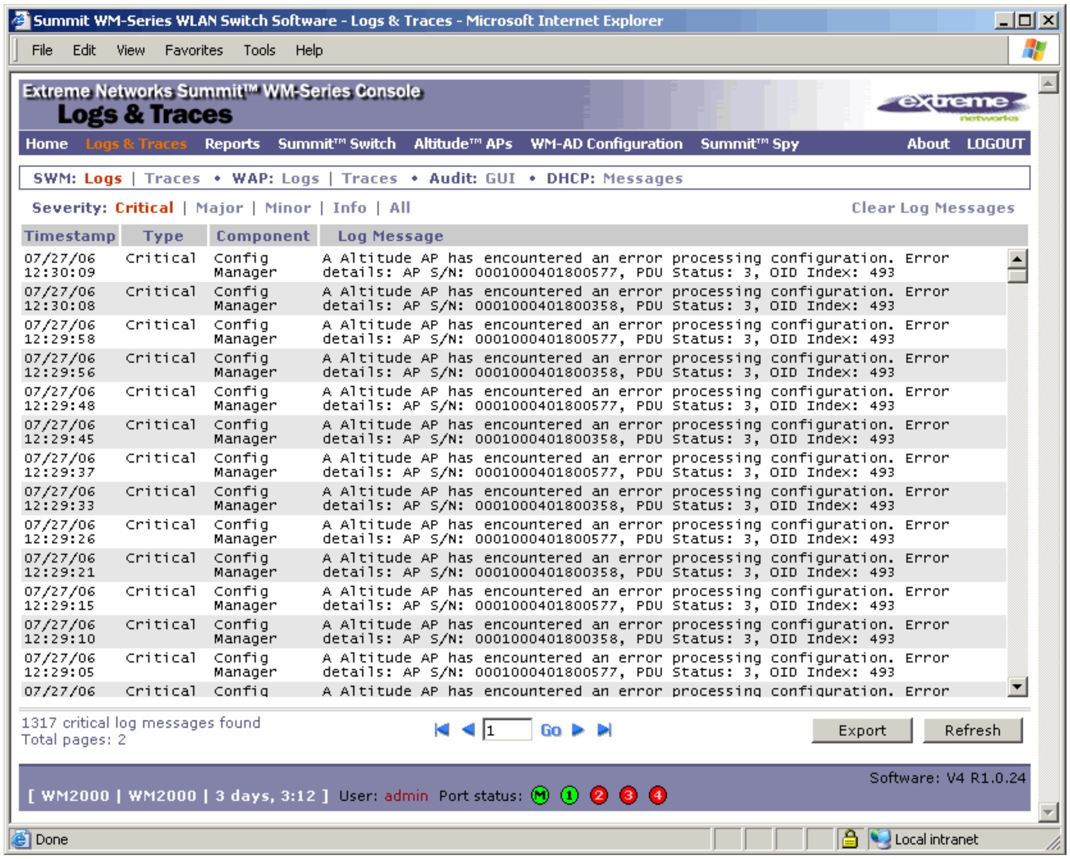
5 To refresh the information in any display, click **Refresh**.

6 To export information from a display as an HTML file, click the **Export** button.

To clear logs:

1 From the main menu, click **Logs & Traces**. The **Logs & Traces** screen is displayed.

2 Click one of the **Log** tabs. The following is an example of the Summit WM series switch logs:


Summit WM-Series WLAN Switch Software - Logs & Traces - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Logs & Traces
extreme networks
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
SWM: Logs | Traces • WAP: Logs | Traces • Audit: GUI • DHCP: Messages
Severity: Critical | Major | Minor | Info | All
Clear Log Messages
1
Go
Export
Refresh
M 1 2 3 4
Done
Local intranet

Timestamp	Type	Component	Log Message
07/27/06 12:30:09	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:30:08	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:29:58	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:29:56	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:29:48	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:29:45	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:29:37	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:29:33	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:29:26	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:29:21	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:29:15	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:29:10	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:29:05	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06	Critical	Config	A Altitude AP has encountered an error processing configuration. Error

1317 critical log messages found
Total pages: 2

Software: V4 R1.0.24

[WM2000 | WM2000 | 3 days, 3:12] User: admin Port status:

The events are displayed in chronological order, sorted by the **Timestamp** column.

3 To clear the logs, click **Clear Log Messages**.

Glossary

Networking terms and abbreviations

A

AAA

Authentication, Authorization and Accounting. A system in IP-based networking to control what computer resources users have access to and to keep track of the activity of users over a network.

Access Point (AP)

A wireless LAN transceiver or "base station" that can connect a wired LAN to one or many wireless devices.

Ad-hoc mode

An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an access point (AP). (Compare Infrastructure Mode)

AES

Advanced Encryption Standard (AES) is an algorithm for encryption that works at multiple network layers simultaneously. As a block cipher, AES encrypts data in fixed-size blocks of 128 bits. AES was created by the National Institute of Standards and Technology (NIST). AES is a privacy transform for IPSec and Internet Key Exchange (IKE). AES has a variable key length - the algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key.

For the WPA2/802.11i implementation of AES, a 128 bit key length is used. AES encryption includes 4 stages that make up one round. Each round is then iterated 10, 12 or 14 times depending upon the bit-key size. For the WPA2/802.11i implementation of AES, each round is iterated 10 times.

AES-CCMP

AES uses the Counter-Mode/CBC-MAC Protocol (CCMP). CCM is a new mode of operation for a block cipher that enables a single key to be used for both encryption and authentication. The two underlying modes employed in CCM include Counter mode (CTR) that achieves data encryption and Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity.

ARP

Address Resolution Protocol. A protocol used to obtain the physical addresses (such as MAC addresses) of hardware units in a network environment. A host obtains such a physical address by broadcasting an ARP request, which contains the IP address of the target hardware unit. If the request finds a unit with that IP address, the unit replies with its physical hardware address.

Association

A connection between a wireless device and an Access Point.

asynchronous

Asynchronous transmission mode (ATM). A start/stop transmission in which each character is preceded by a start signal and followed by one or more stop signals. A variable time interval can exist between characters. ATM is the preferred technology for the transfer of images.

B

BSS

Basic Service Set. A wireless topology consisting of one Access Point connected to a wired network and a set of wireless devices. Also called an infrastructure network. See also IBSS.

C

Captive Portal

A browser-based authentication mechanism that forces unauthenticated users to a Web page. Sometimes called a “reverse firewall”.

CDR

Call Data (Detail) Record

In Internet telephony, a call detail record is a data record that contains information related to a telephone call, such as the origination and destination addresses of the call, the time the call started and ended, the duration of the call, the time of day the call was made and any toll charges that were added through the network or charges for operator services, among other details of the call.

In essence, call accounting is a database application that processes call data from your switch (PBX, iPBX, or key system) via a CDR (call detail record) or SMDR (station message detail record) port. The call data record details your system's incoming and outgoing calls by thresholds, including time of call, duration of call, dialing extension, and number dialed. Call data is stored in a PC database

CHAP

Challenge-Handshake Authentication Protocol. One of the two main authentication protocols used to verify a user's name and password for PPP Internet connections. CHAP is more secure than PAP because it performs a three-way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link has been established.

CLI

Command Line Interface.

Collision

Two Ethernet packets attempting to use the medium simultaneously. Ethernet is a shared media, so there are rules for sending packets of data to avoid conflicts and protect data integrity. When two nodes at different locations attempt to send data at the same time, a collision will result. Segmenting the network with bridges or switches is one way of reducing collisions in an overcrowded network.

D

Datagram

A datagram is “a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.” (RFC1594). The term has been generally replaced by the term packet. Datagrams or packets are the message units that the Internet Protocol deals with and that the Internet transports.

Decapsulation

See tunnelling.

D (Continued)

Device Server

A specialized, network-based hardware device designed to perform a single or specialized set of server functions. Print servers, terminal servers, remote access servers and network time servers are examples of device servers.

DHCP

Dynamic Host Configuration Protocol. A protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocation of network addresses to hosts. (IETF RFC1531.)

Option 78 specifies the location of one or more SLP Directory Agents. Option 79 specifies the list of scopes that a SLP Agent is configured to use.(RFC2610 - DHCP Options for Service Location Protocol)

Directory Agent (DA)

A method of organizing and locating the resources (such as printers, disk drives, databases, e-mail directories, and schedulers) in a network. Using SLP, networking applications can discover the existence, location and configuration of networked devices.

With Service Location Protocol, client applications are 'User Agents' and services are advertised by 'Service Agents'. The User Agent issues a multicast 'Service Request' (SrvRqst) on behalf of the client application, specifying the services required. The User Agent will receive a Service Reply (SrvRply) specifying the location of all services in the network which satisfy the request.

For larger networks, a third entity, called a 'Directory Agent', receives registrations from all available Service Agents. A User Agent sends a unicast request for services to a Directory Agent (if there is one) rather than to a Service Agent.

(SLP version 2, RFC2608, updating RFC2165)

Diversity antenna and receiver

The AP has two antennae. Receive diversity refers to the ability of the AP to provide better service to a device by receiving from the user on which ever of the two antennae is receiving the cleanest signal. Transmit diversity refers to the ability of the AP to use its two antenna to transmit on a specific antenna only, or on a alternate antennae. The antennae are called diversity antennae because of this capability of the pair.

DNS

Domain Name Server

DSSS

Direct-Sequence Spread Spectrum. A transmission technology used in Local Area Wireless Network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. (Compare FHSS)

D (Continued)

DTIM

DTIM delivery traffic indication message (in 802.11 standard)

Dynamic WEP

The IEEE introduced the concept of user-based authentication using per-user encryption keys to solve the scalability issues that surrounded static WEP. This resulted in the 802.1X standard, which makes use of the IETF's Extensible Authentication Protocol (EAP), which was originally designed for user authentication in dial-up networks. The 802.1X standard supplemented the EAP protocol with a mechanism to send an encryption key to an Altitude AP. These encryption keys are used as dynamic WEP keys, allowing traffic to each individual user to be encrypted using a separate key.

E

EAP-TLS
EAP-TTLS

EAP-TLS Extensible Authentication Protocol - Transport Layer Security. A general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards. IEEE 802.1x specifies how EAP should be encapsulated in LAN frames.

In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the access point for proof of identity, which the access point gets from the user and then sends back to the server to complete the authentication.

EAP-TLS provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys.

EAP-TTLS (Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.

(*See also* PEAP)

ELA (OPSEC)

Event Logging API (Application Program Interface) for OPSEC, a module in Check Point used to enable third-party applications to log events into the Check Point VPN-1/FireWall-1 management system.

Encapsulation

See tunnelling.

ESS

Extended Service Set (ESS). Several Basic Service Sets (BSSs) can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). The SSID is used to identify the ESS. (*See* BSS and SSID.)

F

FHSS

Frequency-Hopping Spread Spectrum. A transmission technology used in Local Area Wireless Network (LAWN) transmissions where the data signal is modulated with a narrowband carrier signal that “hops” in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. This technique reduces interference. If synchronized properly, a single logical channel is maintained. (Compare DSSS)

Fit, thin and fat APs

A thin AP architecture uses two components: an access point that is essentially a stripped-down radio and a centralized management controller that handles the other WLAN system functions. Wired network switches are also required.

A fit AP, a variation of the thin AP, handles the RF and encryption, while the central management controller, aware of the wireless users' identities and locations, handles secure roaming, quality of service, and user authentication. The central management controller also handles AP configuration and management.

A fat (or thick) AP architecture concentrates all the WLAN intelligence in the access point. The AP handles the radio frequency (RF) communication, as well as authenticating users, encrypting communications, secure roaming, WLAN management, and in some cases, network routing.

FQDN

Fully Qualified Domain Name. A “friendly” designation of a computer, of the general form computer.[subnetwork.].organization.domain. The FQDN names must be translated into an IP address in order for the resource to be found on a network, usually performed by a Domain Name Server.

FTM

Forwarding Table Manager

FTP

File Transfer Protocol

G

Gateway

In the wireless world, an access point with additional software capabilities such as providing NAT and DHCP. Gateways may also provide VPN support, roaming, firewalls, various levels of security, etc.

Gigabit Ethernet

The high data rate of the Ethernet standard, supporting data rates of 1 gigabit (1,000 megabits) per second.

GUI

Graphical User Interface

H

Heartbeat message

A heartbeat message is a UDP data packet used to monitor a data connection, polling to see if the connection is still alive.
In general terms, a heartbeat is a signal emitted at regular intervals by software to demonstrate that it is still alive. In networking, a heartbeat is the signal emitted by a Level 2 Ethernet transceiver at the end of every packet to show that the collision-detection circuit is still connected.

Host

(1) A computer (usually containing data) that is accessed by a user working on a remote terminal, connected by modems and telephone lines.

(2) A computer that is connected to a TCP/IP network, including the Internet. Each host has a unique IP address.

HTTP

Hypertext Transfer Protocol is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. A Web browser makes use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols. (RFC2616: Hypertext Transfer Protocol -- HTTP/1.1)

HTTPS

Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL, is a Web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS uses Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

IBSS

Independent Basic Service Set. *See* BSS. An IBSS is the 802.11 term for an adhoc network. *See* adhoc network.

ICMP

Internet Control Message Protocol, an extension to the Internet Protocol (IP) defined by RFC792. ICMP supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

ICV

ICV (Integrity Check Value) is a 4-byte code appended in standard WEP to the 802.11 message. Enhanced WPA inserts an 8-byte MIC just before the ICV. (*See* WPA and MIC)

IE

Internet Explorer.

IEEE

Institute of Electrical and Electronics Engineers, a technical professional association, involved in standards activities.

IETF

Internet Engineering Task Force, the main standards organization for the Internet.

I (Continued)

Infrastructure Mode

An 802.11 networking framework in which devices communicate with each other by first going through an Access Point (AP). In infrastructure mode, wireless devices can communicate with each other or can communicate with a wired network. (*See* ad-hoc mode and BSS.)

Internet or IP telephony

IP or Internet telephony are communications, such as voice, facsimile, voice-messaging applications, that are transported over the Internet, rather than the public switched telephone network (PSTN). IP telephony is the two-way transmission of audio over a packet-switched IP network (TCP/IP network).

An Internet telephone call has two steps: (1) converting the analog voice signal to digital format, (2) translating the signal into Internet protocol (IP) packets for transmission over the Internet. At the receiving end, the steps are reversed. Over the public Internet, voice quality varies considerably. Protocols that support Quality of Service (QoS) are being implemented to improve this.

IP

Internet Protocol is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (host) on the Internet has at least one IP address that uniquely identifies it. Internet Protocol specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

IPC

Interprocess Communication. A capability supported by some operating systems that allows one process to communicate with another process. The processes can be running on the same computer or on different computers connected through a network.

IPsec
IPsec-ESP
IPsec-AH

Internet Protocol security (IPSec)

Internet Protocol security Encapsulating Security Payload (IPsec-ESP). The encapsulating security payload (ESP) encapsulates its data, enabling it to protect data that follows in the datagram. Internet Protocol security Authentication Header (IPsec-AH). AH protects the parts of the IP datagram that can be predicted by the sender as it will be received by the receiver. IPsec is a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet. For IPsec to work, the sending and receiving devices must share a public key. This is accomplished through a protocol known as Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows the receiver to obtain a public key and authenticate the sender using digital certificates.

I (Continued)

isochronous

Isochronous data is data (such as voice or video) that requires a constant transmission rate, where data must be delivered within certain time constraints. For example, multimedia streams require an isochronous transport mechanism to ensure that data is delivered as fast as it is displayed and to ensure that the audio is synchronized with the video. Compare: asynchronous processes in which data streams can be broken by random intervals, and synchronous processes, in which data streams can be delivered only at specific intervals.

ISP

Internet Service Provider.

IV

IV (Initialization Vector), part of the standard WEP encryption mechanism that concatenates a shared secret key with a randomly generated 24-bit initialization vector. WPA with TKIP uses 48-bit IVs, an enhancement that significantly increases the difficulty in cracking the encryption. (*See* WPA and TKIP)

L

LAN

Local Area Network.

License installation

LSA

Link State Advertisements received by the currently running OSPF process. The LSAs describe the local state of a router or network, including the state of the router's interfaces and adjacencies. *See* also OSPF.

M

MAC

Media Access Control layer. One of two sublayers that make up the Data Link Layer of the OSI model. The MAC layer is responsible for moving data packets to and from one Network Interface Card (NIC) to another across a shared channel.

MAC address

Media Access Control address. A hardware address that uniquely identifies each node of a network.

MIB

Management Information Base is a formal description of a set of network objects that can be managed using the Simple Network Management Protocol (SNMP). The format of the MIB is defined as part of the SNMP. A MIB is a collection of definitions defining the properties of a managed object within a device. Every managed device keeps a database of values for each of the definitions written in the MIB. Definition of the MIB conforms to RFC1155 (Structure of Management Information).

M (Continued)

MIC

Message Integrity Check or Code (MIC), also called “Michael”, is part of WPA and TKIP. The MIC is an additional 8-byte code inserted before the standard 4-byte integrity check value (ICV) that is appended in by standard WEP to the 802.11 message. This greatly increases the difficulty in carrying out forgery attacks.

Both integrity check mechanisms are calculated by the receiver and compared against the values sent by the sender in the frame. If the values match, there is assurance that the message has not been tampered with. (*See* WPA, TKIP and ICV).

MTU

Maximum Transmission Unit. The largest packet size, measured in bytes, that a network interface is configured to accept. Any messages larger than the MTU are divided into smaller packets before being sent.

MU

Mobile Unit, a wireless device such as a PC laptop.

multicast, broadcast, unicast

Multicast: transmitting a single message to a select group of recipients. Broadcast: sending a message to everyone connected to a network. Unicast: communication over a network between a single sender and a single receiver.

N

NAS

Network Access Server, a server responsible for passing information to designated RADIUS servers and then acting on the response returned. A NAS-Identifier is a RADIUS attribute identifying the NAS server. (RFC2138)

NAT

Network Address Translator. A network capability that enables a group of computers to dynamically share a single incoming IP address. NAT takes the single incoming IP address and creates new IP address for each client computer on the network.

Netmask

In administering Internet sites, a netmask is a string of 0's and 1's that mask or screen out the network part of an IP address, so that only the host computer part of the address remains. A frequently-used netmask is 255.255.255.0, used for a Class C subnet (one with up to 255 host computers). The “.0” in the “255.255.255.0” netmask allows the specific host computer address to be visible.

NIC

Network Interface Card. An expansion board in a computer that connects the computer to a network.

NMS

Network Management System. The system responsible for managing a network or a portion of a network. The NMS talks to network management agents, which reside in the managed nodes.

N (Continued)

NTP

Network Time Protocol, an Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network of computers. Based on UTC, NTP synchronizes client workstation clocks to the U.S. Naval Observatory Master Clocks in Washington, DC and Colorado Springs CO. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client's clock. (RFC1305)

O

OFDM

Orthogonal frequency division multiplexing, a method of digital modulation in which a signal is split into several narrowband channels at different frequencies. OFDM is similar to conventional frequency division multiplexing (FDM). The difference lies in the way in which the signals are modulated and demodulated. Priority is given to minimizing the interference, or crosstalk, among the channels and symbols comprising the data stream. Less importance is placed on perfecting individual channels.

OFDM is used in European digital audio broadcast services. It is also used in wireless local area networks.

OID

Object Identifier.

OPSEC

OPSEC (Open Platform for Security) is a security alliance program created by Check Point to enable an open industry-wide framework for interoperability of security products and applications. Products carrying the “Secured by Check Point” seal have been tested to guarantee integration and interoperability.

OS

Operating system.

OSI

Open System Interconnection. An ISO standard for worldwide communications that defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, down through the presentation, session, transport, network, data link layer to the physical layer at the bottom, over the channel to the next station and back up the hierarchy.

OSI Layer 2

At the Data Link layer (OSI Layer 2), data packets are encoded and decoded into bits. The data link layer has two sublayers:

- the Logical Link Control (LLC) layer controls frame synchronization, flow control and error checking
- The Media Access Control (MAC) layer controls how a computer on the network gains access to the data and permission to transmit it.

OSI Layer 3

The Network layer (OSI Layer 3) provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.

O (Continued)

OSPF

Open Shortest Path First, an interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm. Routers use link-state algorithms to send routing information to all nodes in an internetwork by calculating the shortest path to each node based on a topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations) that describes the state of its own links, and it also sends the complete routing structure (topography). Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately multicasts the information to all other hosts in the network so that all will have the same routing table information. The host using OSPF sends only the part that has changed, and only when a change has taken place. (RFC2328)

OUI

Organizationally Unique Identifier (used in MAC addressing).

P

Packet

The unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into packets. Each packet is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file (by the TCP layer at the receiving end).

PAP

Password Authentication Protocol is the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted. (*See* CHAP).

PDU

Protocol Data Unit. A data object exchanged by protocol machines (such as management stations, SMUX peers, and SNMP agents) and consisting of both protocol control information and user data. PDU is sometimes used as a synonym for “packet''.

PEAP

PEAP (Protected Extensible Authentication Protocol) is an IETF draft standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user. If the first phase is successful, the user is then authenticated over the SSL tunnel created in phase one using EAP-Generic Token Card (EAP-GTC) or Microsoft Challenged Handshake Protocol Version 2 (MSCHAP V2). (*See* also EAP-TLS).

PHP server

Hypertext Preprocessor

PKI

Public Key Infrastructure

P (Continued)

PoE

Power over Ethernet. The Power over Ethernet standard (802.3af) defines how power can be provided to network devices over existing Ethernet connection, eliminating the need for additional external power supplies.

POST

Power On Self Test, a diagnostic testing sequence performed by a computer to determine if its hardware elements are present and powered on. If so, the computer begins its boot sequence.

push-to-talk (PTT)

The push-to-talk (PTT) is feature on wireless telephones that allows them to operate like a walkie-talkie in a group, instead of standard telephone operation. The PTT feature requires that the network be configured to allow multicast traffic.

A PTT call is initiated by selecting a channel and pressing the “talk” key on the wireless telephone. All wireless telephones on the same network that are monitoring the channel will hear the transmission. On a PTT call you hold the button to talk and release it to listen.

Q

QoS

Quality of Service. A term for a number of techniques that intelligently match the needs of specific applications to the network resources available, using such technologies as Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks. QoS features provide better network service by supporting dedicated bandwidth, improving loss characteristics, avoiding and managing network congestion, shaping network traffic, setting traffic priorities across the network.
Quality-of-Service (QoS): A set of service requirements to be met by the network while transporting a flow. (RFC2386)

R

RADIUS

Remote Authentication Dial-In User Service. An authentication and accounting system that checks User Name and Password and authorizes access to a network. The RADIUS specification is maintained by a working group of the IETF (RFC2865 RADIUS, RFC2866 RADIUS Accounting, RFC2868 RADIUS Attributes for Tunnel Protocol Support).

RF

Radio Frequency, a frequency in the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that can propagate through space. These frequencies in the electromagnetic spectrum range from Ultra-low frequency (ULF) -- 0-3 Hz to Extremely high frequency (EHF) -- 30GHz - 300 GHz. The middle ranges are: Low frequency (LF) -- 30 kHz - 300 kHz, Medium frequency (MF) -- 300 kHz - 3 MHz, High frequency (HF) -- 3MHz - 30 MHz, Very high frequency (VHF) -- 30 MHz - 300 MHz, Ultra-high frequency (UHF)-- 300MHz - 3 GHz.

R (Continued)

RFC

Request for Comments, a series of notes about the Internet, submitted to the Internet Engineering Task Force (IETF) and designated by an RFC number, that may evolve into an Internet standard. The RFCs are catalogued and maintained on the IETF RFC website: www.ietf.org/rfc.html.

Roaming

In 802.11, roaming occurs when a wireless device (a station) moves from one Access Point to another (or BSS to another) in the same Extended Service Set (ESS) -identified by its SSID.

RP-SMA

Reverse Polarity-Subminiature version A, a type of connector used with wireless antennas

RSN

Robust Security Network. A new standard within IEEE 802.11 to provide security and privacy mechanisms. The RSN (and related TSN) both specify IEEE 802.1x authentication with Extensible Authentication Protocol (EAP).

RSSI

RSSI received signal strength indication (in 802.11 standard)

RTS / CTS

RTS request to send, CTS clear to send (in 802.11 standard)

S

Segment

In Ethernet networks, a section of a network that is bounded by bridges, routers or switches. Dividing a LAN segment into multiple smaller segments is one of the most common ways of increasing available bandwidth on the LAN.

SLP

Service Location Protocol. A method of organizing and locating the resources (such as printers, disk drives, databases, e-mail directories, and schedulers) in a network. Using SLP, networking applications can discover the existence, location and configuration of networked devices.

With Service Location Protocol, client applications are 'User Agents' and services are advertised by 'Service Agents'. The User Agent issues a multicast 'Service Request' (SrvRqst) on behalf of the client application, specifying the services required. The User Agent will receive a Service Reply (SrvRply) specifying the location of all services in the network which satisfy the request.

For larger networks, a third entity, called a 'Directory Agent', receives registrations from all available Service Agents. A User Agent sends a unicast request for services to a Directory Agent (if there is one) rather than to a Service Agent.

(SLP version 2, RFC2608, updating RFC2165)

SMI

Structure of Management Information. A hierarchical tree structure for information that underlies Management Information Bases (MIBs), and is used by the SNMP protocol. Defined in RFC1155 and RFC1442 (SNMPv2).

S (Continued)

SMT (802.11)

Station ManagemenT. The object class in the 802.11 MIB that provides the necessary support at the station to manage the processes in the station such that the station may work cooperatively as a part of an IEEE 802.11 network. The four branches of the 802.11 MIB are:

- dot11smt - objects related to station management and local configuration
- dot11mac - objects that report/configure on the status of various MAC parameters
- dot11res - Objects that describe available resources
- dot11phy - Objects that report on various physical items.

SNMP

Simple Network Management Protocol. A set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

SNMP includes a limited set of management commands and responses. The management system issues Get, GetNext and Set messages to retrieve single or multiple object variables or to establish the value of a single variable. The managed agent sends a Response message to complete the Get, GetNext or Set.

SNMP trap

An event notification sent by the SNMP managed agent to the management system to identify the occurrence of conditions (such as a threshold that exceeds a predetermined value).

SSH

Secure Shell, sometimes known as Secure Socket Shell, is a Unix-based command interface and protocol for securely getting access to a remote computer. SSH is a suite of three utilities - slogin, ssh, and scp - secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. With SSH commands, both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

SSID

Service Set Identifier. A 32-character unique identifier attached to the header of packets sent over a Wireless LAN that acts as a password when a wireless device tries to connect to the Basic Service Set (BSS). Several BSSs can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). The SSID is used to identify the ESS.

In 802.11 networks, each Access Point advertises its presence several times per second by broadcasting beacon frames that carry the ESS name (SSID). Stations discover APs by listening for beacons, or by sending probe frames to search for an AP with a desired SSID. When the station locates an appropriately-named Access Point, it sends an associate request frame containing the desired SSID. The AP replies with an associate response frame, also containing the SSID.

Some APs can be configured to send a zero-length broadcast SSID in beacon frames instead of sending their actual SSID. The AP must return its actual SSID in the probe response.

S (Continued)

SSL

Secure Sockets Layer. A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. URLs that require an SSL connection start with https: instead of http.

SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL.

Subnet mask

(*See* netmask)

Subnets

Portions of networks that share the same common address format. A subnet in a TCP/IP network uses the same first three sets of numbers (such as 198.63.45.xxx), leaving the fourth set to identify devices on the subnet. A subnet can be used to increase the bandwidth on the network by breaking the network up into segments.

SVP

SpectraLink Voice Protocol, a protocol developed by SpectraLink to be implemented on access points in order to facilitate voice prioritization over an 802.11 wireless LAN that will carry voice packets from SpectraLink wireless telephones.

Switch

In networks, a device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model and therefore support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.

syslog

A protocol used for the transmission of event notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, and now embedded in many other operating systems and networked devices. A device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.

Syslog uses the user datagram protocol (UDP) as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC3164)

T

TCP / IP

Transmission Control Protocol. TCP, together with IP (Internet Protocol), is the basic communication language or protocol of the Internet. Transmission Control Protocol manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. Internet Protocol handles the address part of each packet so that it gets to the right destination.

TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network.

TFTP

Trivial File Transfer Protocol. An Internet software utility for transferring files that is simpler to use than the File Transfer Protocol (FTP) but less capable. It is used where user authentication and directory visibility are not required. TFTP uses the User Datagram Protocol (UDP) rather than the Transmission Control Protocol (TCP). TFTP is described formally in Request for Comments (RFC) 1350.

TKIP

Temporal Key Integrity Protocol (TKIP) is an enhancement to the WEP encryption technique that uses a set of algorithms that rotates the session keys. TKIPs' enhanced encryption includes a per-packet key mixing function, a message integrity check (MIC), an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. The encryption keys are changed (rekeyed) automatically and authenticated between devices after the rekey interval (either a specified period of time, or after a specified number of packets has been transmitted).

TLS

Transport Layer Security. (*See* EAP, Extensible Authentication Protocol)

ToS / DSCP

ToS (Type of Service) / DSCP (Diffserv Codepoint). The ToS/DSCP box contained in the IP header of a frame is used by applications to indicate the priority and Quality of Service (QoS) for each frame. The level of service is determined by a set of service parameters which provide a three way trade-off between low-delay, high-reliability, and high-throughput. The use of service parameters may increase the cost of service.

TSN

Transition Security Network. A subset of Robust Security Network (RSN), which provides an enhanced security solution for legacy hardware. The Wi-Fi Alliance has adopted a solution called Wireless Protected Access (WPA), based on TSN. RSN and TSN both specify IEEE 802.1x authentication with Extensible Authentication Protocol (EAP).

Tunnelling

Tunnelling (or encapsulation) is a technology that enables one network to send its data via another network's connections. Tunnelling works by encapsulating packets of a network protocol within packets carried by the second network. The receiving device then decapsulates the packets and forwards them in their original format.

U

UDP

User Datagram Protocol. A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive packets over an IP network. It is used primarily for broadcasting messages over a network.

U-NII

Unlicensed National Information Infrastructure. Designated to provide short-range, high-speed wireless networking communication at low cost, U-NII consists of three frequency bands of 100 MHz each in the 5 GHz band: 5.15-5.25GHz (for indoor use only), 5.25-5.35 GHz and 5.725-5.825GHz. The three frequency bands were set aside by the FCC in 1997 initially to help schools connect to the Internet without the need for hard wiring. U-NII devices do not require licensing.

URL

Uniform Resource Locator. the unique global address of resources or files on the World Wide Web. The URL contains the name of the protocol to be used to access the file resource, the IP address or the domain name of the computer where the resource is located, and a pathname -- a hierarchical description that specifies the location of a file in that computer.

V

VoIP

Voice Over Internet Protocol. An internet telephony technique. With VoIP, a voice transmission is cut into multiple packets, takes the most efficient path along the Internet and is reassembled when it reaches the destination.

VPN

Virtual Private Network. A private network that is constructed by using public wires to connect nodes. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

VSA

Vendor Specific Attribute, an attribute for a RADIUS server defined by the manufacturer.(compared to the RADIUS attributes defined in the original RADIUS protocol RFC2865). A VSA attribute is defined in order that it can be returned from the RADIUS server in the Access Granted packet to the Radius Client.

W

Walled Garden

A restricted subset of network content that wireless devices can access.

WEP

Wired Equivalent Privacy. A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.

Wi-Fi

Wireless fidelity. A term referring to any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. Used in reference to the Wi-Fi Alliance, a nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification.

W (Continued)

WINS

Windows Internet Naming Service. A system that determines the IP address associated with a particular network computer, called name resolution. WINS supports network client and server computers running Windows and can provide name resolution for other computers with special arrangements. WINS supports dynamic addressing (DHCP) by maintaining a distributed database that is automatically updated with the names of computers currently available and the IP address assigned to each one.

DNS is an alternative system for name resolution suitable for network computers with fixed IP addresses.

WLAN

Wireless Local Area Network.

WM-AD

WM Access Domain Services (WM-AD). Extreme Networks' means of mapping wireless networks to the topology of an existing wired network. When you set up WM-AD on the Summit WM series switch, you are defining subnets for groups of wireless users. This WM-AD definition creates a virtual IP subnet where the Summit WM series switch acts as a default gateway for wireless devices. This technique enables policies and authentication to be applied to the groups of wireless users on a WM-AD, as well as the collecting of accounting information. When a WM-AD is set up on the Summit WM series switch, one or more Altitude APs (by radio) are associated with it. A range of IP addresses is set aside for the Summit WM series switch's DHCP server to assign to wireless devices.

WMM

Wi-Fi Multimedia (WMM), a Wi-Fi Alliance certified standard that provides multimedia enhancements for Wi-Fi networks that improve the user experience for audio, video, and voice applications. This standard is compliant with the IEEE 802.11e Quality of Service (QoS) extensions for 802.11 networks. WMM provides prioritized media access by shortening the time between transmitting packets for higher priority traffic. WMM is based on the Enhanced Distributed Channel Access (EDCA) method.

WPA

Wireless Protected Access, or Wi-Fi Protected Access is a security solution adopted by the Wi-Fi Alliance that adds authentication to WEPs' basic encryption. For authentication, WPA specifies IEEE 802.1x authentication with Extensible Authentication Protocol (EAP). For encryption, WPA uses the Temporal Key Integrity Protocol (TKIP) mechanism, which shares a starting key between devices, and then changes their encryption key for every packet. Certificate Authentication (CA) can also be used. Also part of the encryption mechanism are 802.1X for dynamic key distribution and Message Integrity Check (MIC) a.k.a. Michael.

WPA requires that all computers and devices have WPA software.

W (Continued)

WPA-PSK

Wi-Fi Protected Access with Pre-Shared Key, a special mode of WPA for users without an enterprise authentication server. Instead, for authentication, a Pre-Shared Key is used. The PSK is a shared secret (passphrase) that must be entered in both the Altitude AP or router and the WPA clients.

This preshared key should be a random sequence of characters at least 20 characters long or hexadecimal digits (numbers 0-9 and letters A-F) at least 24 hexadecimal digits long. After the initial shared secret, the Temporal Key Integrity Protocol (TKIP) handles the encryption and automatic rekeying.

Summit WM series switch, access points, and WLAN switch software terms and abbreviations

Term — **Explanation**

Altitude AP

The Altitude AP is a wireless LAN thin access point (IEEE 802.11) provided with unique software that allows it to communicate only with a Summit WM series switch. (A thin access point handles the radio frequency (RF) communication but relies on a controller to handle WLAN elements such as authentication.) The Altitude AP also provides local processing such as encryption. The Altitude AP is a dual-band access point, with both 802.11a and 802.11b/g radios.

CTP

CAPWAP Tunnelling Protocol (CTP). The Altitude AP uses a UDP (User Datagram Protocol) based tunnelling protocol called CAPWAP Tunnelling Protocol (CTP) to encapsulate the 802.11 packets and forward them to the Summit WM series switch.

The CTP protocol defines a mechanism for the control and provisioning of Altitude APs (CAPWAP) through centralized access controllers. In addition, it provides a mechanism providing the option to tunnel the mobile client data between the access point and the access controller.

Data Collector

The Data Collector is an application on the Summit WM series switch that receives and manages the Radio Frequency (RF) scan messages sent by the Altitude AP. This application is part of the Summit spy technique, working in conjunction with the scanner mechanism and the Analysis Engine to assist in detecting rogue access points.

DRM (dynamic radio/RF management)

The DRM feature consists of software on the Altitude AP that provides dynamic radio frequency (RF) management. For Altitude APs with the DRM feature enabled and on a common channel, the power levels will be adjusted to balance coverage if an Altitude AP is added to, or leaves, the network. The feature also allows wireless clients to be moved to another Altitude AP if the load is too high. The feature can also be set to scan automatically for a channel, using a channel selection algorithm.

Langley

Langley is a Summit WM series switch, access points, and WLAN switch software term for the inter-process messaging infrastructure on the Summit WM series switch.

Mobility manager (and mobility agent)

The technique in Summit WM series switch, access points, and WLAN switch software by which multiple Summit WM series switches on a network can discover each other and exchange information about a client session. This enables a wireless device user to roam seamlessly between different Altitude APs on different Summit WM series switches, to provide mobility to the wireless device user.

One Summit WM series switch on the network must be designated as the mobility manager. All other Summit WM series switches are designated as mobility agents. Relying on SLP, the mobility manager registers with the Directory Agent and the mobility agents discover the location of the mobility manager.

Summit WM series switch

The Summit WM series switch is a rack-mountable network device designed to be integrated into an existing wired Local Area Network (LAN). It provides centralized control over all access points (both Altitude APs and third-party access points) and manages the network assignment of wireless device clients associating through access points.

Summit spy

The Summit spy is a mechanism that assists in the detection of rogue access points. The feature has three components: (1) a radio frequency (RF) scanning task that runs on the Altitude AP, (2) an application called the Data Collector on the Summit WM series switch that receives and manages the RF scan messages sent by the Altitude AP, (3) an Analysis Engine on the Summit WM series switch that processes the scan data.

WM-AD

WM Access Domain Services (WM-AD). Extreme Networks' means of mapping wireless networks to the topology of an existing wired network. When you set up WM-AD on the Summit WM series switch, you are defining subnets for groups of wireless users. This WM-AD definition creates a virtual IP subnet where the Summit WM series switch acts as a default gateway for wireless devices. This technique enables policies and authentication to be applied to the groups of wireless users on a WM-AD, as well as the collecting of accounting information. When a WM-AD is set up on the Summit WM series switch, one or more Altitude APs (by radio) are associated with it. A range of IP addresses is set aside for the Summit WM series switch's DHCP server to assign to wireless devices.

A System states and LEDs

Summit WM series switch system states and LEDs

The Summit WM series switch has the two system states: Standby and Active.

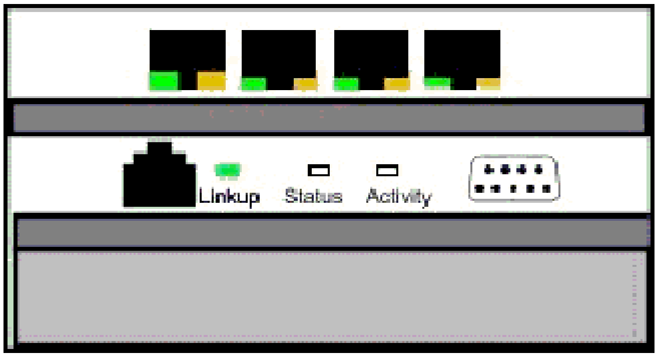
It enters Standby state when shut down in the user interface. During this state, the Summit WM series switch:

- sends a control message to Altitude APs to enter Standby state
- does not handle any wireless traffic or sessions
- disables DHCP, Policy Manager, Security Manager, Altitude AP Manager, and Redirector
- remains on the wired network

The Summit WM series switch enters Active state on startup in the user interface. It responds to the Altitude AP's discover message by returning a message indicating that the Altitude AP can enter the active state.

Activity and traffic monitoring

The activity and traffic on the Summit WM series switch is monitored via three LEDs on the back of the Summit WM series switch. These LEDs are Link, Status, and Activity.



The three LEDs perform the following functions:

- Link LED: Displays the link status of management port Ethernet link as seen by the system software. This LED is only visible at the back of the Summit WM series switch
- Status LED: Indicates the state of the controller from software point of view, normal operation, whether processes have gone down, are restarting, and so on. This LED is visible from both the front and the back of the Summit WM series switch.
- Activity LED: Indicates the amount of traffic carried to and from Altitude APs. This LED is visible from both the front and the back of the Summit WM series switch.

Table 18 shows the sequence of the Status and Activity LEDs.

Table 18: Status and Activity LED sequence

System State	Status LED	Activity LED
Power up	Off	Off
Services started: WDTSTAT installed (init.d starts services)	Blinking Amber	Off
Startup Manager Task started	Solid Amber	Blinking Amber
Startup Manager Task completes startup – all components started	Solid Green	Blinking green, if traffic Blank, if no traffic
A component fails to start or needs restarting (Startup Manager Task retrying that component)	Solid Amber	Blinking green
Summit WM series switch fails to boot	Solid Red	Off
A component fails (no more retries)	Solid Red	Off
System about to be reset by watchdog	Blinking Red	Off

Altitude AP system states

For the Altitude AP, the Status LED in the center also indicates power. The Status LED is dark when unit is off and is green (solid) when the AP has completed discovery and is operational.

The chart below shows states and corresponding Status LED displays:

Table 19: Altitude AP system states and status LED displays

State / Process	Description	LEDs
Power	Altitude AP not powered.	Off
Power	Start up: Power On Self Test (POST)	Steady green (briefly)
Power	Power On Self Test (POST) successful	Off (briefly)
Discovery	If the POST self test is successful, the AP begins Discovery process. Altitude AP is powered on and searching for an active Summit WM series switch. It sends a discover message and waits for a response	Orange (steady)
Fail to find DHCP	Altitude AP failed to find DHCP (will stay in this state until a route appears).	Red-orange (alternate blink)
Failed discovery	If there are SLP issues in failed discovery, the LED display changes.	Green-orange (alternate blink)
Registration	Altitude AP learns the Summit WM series switch's IP address, and can begin the Registration process	Orange (blink)
Failed Registration	Altitude AP fails to learn the Summit WM series switch's IP address.	Red (blink)
Standby	1 Altitude AP enters this state from Discovery when it encounters an active Summit WM series switch and completes the Registration process. 2 Altitude AP enters this state from Active when it receives a control message from the Summit WM series switch to enter this state. If the Altitude AP has any wireless device traffic, it will drop the traffic.	Green (blink)
	Altitude AP fails to register. It will wait 5 seconds and try again.	Red (slow blink)
	Firmware download from the Summit WM series switch is in progress	Orange + green (blink)

Table 19: Altitude AP system states and status LED displays (Continued)

State / Process	Description	LEDs
Active (Ready)	Altitude AP has received a control message from an active Summit WM series switch to enter active or ready state. It is ready to receive wireless traffic. Note: The two Traffic LEDs on either side of the Status LED display a green (blink) if there is active wireless traffic. The left LED is for the 2.4 GHz radio. The right LED is for the 5 GHz radio.	Green (steady)
Vulnerable time interval	Vulnerable time interval (the Summit WM series switch resets to factory default if powered-off for three consecutive times during this state). No vulnerable period when access point is resetting to factory defaults.	Left: Green/Off Center: Off/Green Right: Green/Off
Upgrading firmware	Altitude AP is upgrading its firmware	Center: Red/Green

B Regulatory Information

This section provides the regulatory information for the Summit WM 200/2000 series switch and Altitude 350-2 Access Point.

Configuration of the Altitude 350-2 frequencies and power output are controlled by the regional software purchased with the Summit WM series switch and are downloaded from the sever upon initial set-up. A company is only allowed to download the software related it it's geographic location, thus allowing the proper set-up of Access points in accordance with local laws and regulation. The Altitude 350-2 AP must not be operated until proper regional software is downloaded and properly configured.

NOTE

Please refer to http://www.extremenetworks.com/go/rfcertification.htm for latest regulatory information regarding operation of the Altitude 350-2 Access Point.

Only authorized Extreme Networks service personnel are permitted to service the system. Procedures that should be performed only by Extreme Networks personnel are clearly identified in this guide.

Changes or modifications made to the Summit WM series switch or the Altitude APs which are not expressly approved by Extreme and party responsible for compliance upon installation could void the user's authority to operate the equipment.

Summit WM200 (15955), Summit WM2000 (15956)

Safety Standards

North American Safety of ITE:

- UL 60950-1:2003 1st Ed., Listed Device (US)
- CSA 22.2#60950-1-03 1st Ed. (Canada)

European Safety of ITE:

- EN60950-1:2001+A11
- TUV-R GS Mark by German Notified Body
- 73/23/EEC Low Voltage Directive

International Safety of ITE:

- CB Report & Certificate per IEC 60950-1:2001+ Country Deviations
- AS/NZX 3260 (Australia /New Zealand)

EMI/EMC Standards

North America EMC for ITE:

- FCC CFR 47 part 15 Class A (USA)
- ICES-003 Class A (Canada)

European EMC standards

- EN 55022:1998 Class A
- EN 55024:1998 Class A
  includes IEC 61000-4-2, 3, 4, 5, 6, 11
- EN 61000-3-2,3 (Harmonics & Flicker)
- ETSI EN 300 386:2001 (EMC Telecommunications)
- 89/336/EEC EMC Directive

International EMC Certifications:

- CISPR 22:1997 Class A (International Emissions)
- CISPR 24:1997 Class A (International Immunity)
- IEC/EN 61000-4-2 Electrostatic Discharge, 8kV Contact, 15kV Air, Criteria A
- IEC/EN 61000-4-3 Radiated Immunity 10V/m, Criteria A
- IEC/EN 61000-4-4 Transient Burst, 1kV, Criteria A
- IEC/EN 61000-4-5 Surge, 2kV L-L, 2kV L-G, Level 3, Criteria A
- IEC/EN 61000-4-6 Conducted Immunity, 0.15-80MHz, 10V/m unmod. RMS, Criteria A
- IEC/EN 61000-4-11 Power Dips & Interruptions, >30%, 25 periods, Criteria C

Country Specific:

- VCCI Class A (Japan Emissions)
- AS/NZS 3548 ACA (Australia Emissions)
- CNS 13438:1997 Class A (BSMI-Taiwan)
- NOM/NYCE (Mexico)
- ANATEL (Brazil)
- Argentina Form B
- MIC Mark, EMC Approval (Korea)

Telecom Standards

- ETSI EN 300 386:2001 (EMC Telecommunications)
- ETSI EN 300 019 (Environmental for Telecommunications)

Physical and Environmental

Product Dimensions:

- Width: 17.3 inches (44 cm)
- Depth: 13 inches (33 cm)-with module levers
- Height: 4.4 inches (11.1 cm)-2.5U rack according to IEC 60297-5-100 and IEC 60297-5-107 for front mounted modules

Product Weight:

- 21 lbs (9.4 kg)-with dual PSU

Package Dimensions:

- Width: 25.2 inches (63.5 cm)
- Depth: 18.1 inches (46 cm)
- Height: 9.4 inches (24 cm)

Package Weight:

- 27 lbs (12.3 kg)

Environmental Operating Conditions for Summit WM100/1000, Summit WM200/2000, and Altitude 350-2 AP

Environmental Standards:

- EN/ETSI 300 019-2-1 v2.1.2 - Class 1.2 Storage
- EN/ETSI 300 019-2-2 v2.1.2 - Class 2.3 Transportation
- EN/ETSI 300 019-2-3 v2.1.2 - Class 3.1e Operational
- EN/ETSI 300 753 (1997-10) - Acoustic Noise
- ASTM D3580 Random Vibration Unpackaged 1.5G

Operational Environment:

● Operating Temperature Range.	0 C to +40 C (32° F to 104° F)
● Operating Relative Humidity[1]	10 - 90% RH
● Operating Altitude	0 – 3000 meters (9,850 ft)
● Operating Shock (In Rack)[1]	3G, 11ms, 60 shocks
● Operational Office Vibration (In Rack)[1]	5-100-5 Hz @ 2/10G, 0-Peak, 1 Oct./min.
● Operational Random Vibration[1]	3-500 Hz @ 1.5G rms

[1] Worst-case operational condition. Not for extended use under this condition.

Storage & Transportation Environment:

● Storage & Transportation Temp.Range[1]	–40º C to +70º C (-40º F to 158º F)
● Storage & Transportation Relative Humidity[1]	10 - 95% RH
● Storage & Transportation Shock[1]	18G @ 6ms, 600 shocks (package < 50kg)
● Storage & Transportation Random Vib.[1]	5-20 Hz @ 1.0 ASD w/-3dB/oct. from 20-200 Hz
● Storage & Transportation Packaging Drop[1]	14 drops min on sides & corners @ 39.4” (<15kg box)

Altitude 350-2i Integrated Antenna AP (15938), Altitude 350-2d Detachable Antenna AP (15939)

The Altitude 350-2 AP is Wi-Fi certified for operation in accordance with IEEE 802.11a/b/g. Certification# WFA3822.

NOTE

Operation in the European Community and rest of the world may be dependant on securing local licenses/certifications/regulatory approvals. For details and information on the most recent country-specific requirements for the Altitude 350-2 AP, go to the following website: http://www.extremenetworks.com/go/rfcertification.htm.

United States - FCC Declaration of Conformity Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential and business environment. This equipment generates, uses, and radiates radio frequency energy, and if not installed and used in accordance with instructions, may cause harmful interference. However, there is no guarantee that interference will not occur. If this equipment does cause harmful interference, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the transceiver antenna.
- Increase the distance between the equipment and transceiver.

[1] Worst-case Storage & Transportation condition.

- Connect the equipment to an outlet on a circuit different from that to which the effected equipment is connected.
- Consult the dealer or an experienced radio/TV technician for suggestion.

This equipment meets the conformance standards listed in Table 20.

Table 20: USA Conformance Standards

Safety	• UL 60950-1:2001 1st Edition, Listed Accessory	• UL 2043 Plenum Rated
EMC	• FCC CFR 47 Part 15 Class B	FC Tested To Comply With FCC Standards FCC ID#: RJF-A3502A
Radio Transceiver	• CFR 47 Part 15.247, Class C, 2.4 GHz • CFR 47 Part 15.407, Class C, 5 GHz • CFR 47 Part 15.205, 15.207, 15.209 • CFR 47 Part 2.1091, 2.1093 • FCC OET No. 65 1997	Other: • IEEE 802.11a (5 Ghz) • IEEE 802.11b/g (2.4 GHz) • IEEE 802.3af • FCC ID: RJF-A3502A
Environmental	See Environmental Conditions.	

NOTE

The Altitude 350-2 AP must be installed and used in strict accordance with the manufacture's instructions as described in this guide and the quick start guide for the device to which Altitude 350-2 AP is connected. Any other installation or use of the product violates FCC Part 15 regulations.

NOTE

Operation of the Altitude 350-2 AP is restricted for indoor use only, in the UNII 5.15 - 5.25 GHz band in accordance with 47 CFR 15.407(e).

CAUTION

This Part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using integrated antennas or other Extreme Networks certified antennas. Any changes or modification to the product not expressly approved by Extreme Networks could void the user's authority to operate this device.

Conditions Under Which a Second party may replace a Part 15 Unlicensed Antenna

Second party antenna replacement (end user or second manufacturer) is permitted under the conditions listed below, with no testing or filing requirement. The general technical requirement of FCC Part 15.15 (a)(b)(c) still applies, however.

- Replacement antennas must be equal or lower then 4dBi gain within 2.4Ghz range and 5dB gain within 5GHz range. The replacement antenna must be of same type (Omnidirectional Tri band with Reverse SMA connectors) as previously authorized by the Commission/TCB.

- Replacement antennas must be the same pattern type (i.e. similar in-band and out-of-band antenna beam patterns). Special care must be taken when adhering to this condition; the antenna beam patterns of the antennas tested must be compared with the beam patterns of the replacement antennas for similarities.
- Integral and detachable antennas included with the Altitude 350-2 AP have been tested and included within the FCC/TCB grant. Any other antennas used with the Altitude 350-2 AP must follow these guidelines to be used legally with the Altitude 350-2 AP.
- Antennas offered for sale by Extreme Networks have been tested using the highest gain of each antenna type at maximum output power.

FCC RF Radiation Exposure Statement

The Altitude 350-2 Access Point complies with FCC RF radiated exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This device has been tested and has demonstrated compliance when simultaneously operated in the 2.4 GHz and 5 GHz frequency ranges. This device must not be co-located or operated in conjunction with any other antenna or transmitter.

NOTE

The radiated output power of the Altitude 350-2 APs far below the FCC radio frequency exposure limits as specified in "Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields" (OET Bullet 65, Supplement C). This equipment should be installed and operated with a minimum distance of 20 centimeters (8 inches) between the radiator and your body or other co-located operating antennas.

Department of Communications Canada Compliance Statement

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of the Department of Communications.

Cet appareil numerique respecte les limites de bruits radioelectriques applicables aux appareils numeriques de Classe B prescrites dans la norme sur le materiel brouilleur: "Appareils Numeriques," NMB-003 edictee par le ministere des Communications.

This device complies with Part 15 of the FCC Rules and Canadian Standard RSS-210. Operation is subject to the following conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. This Class B device digital apparatus complies with Canada ICES-003.

This equipment meets the following conformance standards:

Table 21: Canada Conformance Standards

Safety	• cULus Listed Accessory #60950-1-03 1st edition	• Plenum Rated Enclosure
EMC	• ICES-003 Class B	
Radio Transceiver	• RSS-210 • RSS-139-1 • RSS-102 FR Exposure • ID# 4141A-3502	Other: • IEEE 802.11a (5 GHz) • IEEE 802.11b/g (2.4 GHz) • IEEE 802.3af
Environmental	See Environmental Conditions.	

- Operation in the 5150-5250 MHz band is limited to indoor use only to reduce potential for harmful interference to co-channel mobile satellite systems.
- The maximum antenna gain permitted for operation in the 5250-5350 MHz band to comply with the e.i.r.p. limit is 4.3 dBi for the internal antenna and 5 dBi for the external antenna.
- The maximum antenna gain permitted for operation in the 5725-5825 MHz band to comply with the e.i.r.p. limit is 4.3 dBi for the internal antenna and 5 dBi for the external antenna.
- Please note that high power radars are allocated as primary users (meaning they have priority) in the 5250-5350 MHz and 5650-5850 MHz bands and these radars could cause interference and/or damage to LE-LAN devices.

European Community

The Altitude 350-2 APs are wireless ports designed for use in the European Union and other countries with similar regulatory restrictions where the end user or installer is allowed to configure the wireless port for operation by entry of a country code relative to a specific country. Upon connection to the switch the software will prompt the user to enter a country code. After the country code is entered, the switch will set up the wireless port with the proper frequencies and power outputs for that country code.

Declaration of Conformity with regard to R&TTE Directive of the European Union 1999/5/EC

The symbol CE0891(!) indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). The Altitude 350-2i Integral Antenna AP (15938) and Altitude 350-2d Detachable Antenna AP (15939) models meet the following conformance standards.

Table 22: European Conformance Standards

Safety	• 73/23/EEC Low Voltage Directive (LVD) • CB Scheme, IEC 60950-1:2001 with all available country deviations	• GS Mark, EN 60950-1:2001 • Plenum Rated Enclosure
EMC	• 89/336/EEC EMC Directive	
	Emissions	
	• EN55022:1998 Class B • CISPR22:1997 Class B	• EN61000-3-2 and 3-3 • EN/ETSI 301 489-17 (9-2000)
	Immunity	
	• EN55024:1998 Class A, includes IEC 61000-4-2,3,4,5,6,11 • EN/ETSI 301 489-17 (9-2000)	
Radio Transceiver	• R&TTE Directive 1999/5/EC • ETSI/EN 300 328-2 2003-04 (2.4 GHz) • ETSI/EN 301 893-1 2002-07 (5 GHz) • ETSI/EN 301 489-1 2002-08 • ETSI/EN 301 489-17 2002-08 (RLAN)	Other: • IEEE 802.11a (5 Ghz) • IEEE 802.11b/g (2.4 GHz • IEEE 802.3af
Environmental	• EN/ETSI 300 019-2-1 v2.1.2 - Class 1.2 Storage • EN/ETSI 300 019-2-2 v2.1.2 - Class 2.3 Transportation • EN/ETSI 300 019-2-3 v2.1.2 - Class 3.1e Operational • ASTM D5276 Drop Packaged • ASTM D3580 Random Vibration Unpackaged 1.5 G	

NOTE

A signed copy of the Declaration of Conformity (DoC) in accordance with the preceding directives and standards has been made and is available at www.extremenetworks.com/go/rfcertification.htm.

Conditions of Use in the European Community

The Altitude 350-2 Access Point with integrated and detachable antennas is designed and intended to be used indoors. Some EU countries allow outdoor operation with limitations and restrictions, which are described in this section. If the end user chooses to operate the Altitude 350-2 AP outdoors, it is their responsibility to insure operation in accordance with these rules, frequencies, and power output. The Altitude 350-2 AP must not be operated until proper regional software is downloaded.

WARNING!

The user or installer is responsible to ensure that the Altitude 350-2 AP is operated according to channel limitations, indoor / outdoor restrictions, license requirements, and within power level limits for the current country of operation. A configuration utility has been provided with the switch to allow the end user to check the configuration and make necessary configuration changes to ensure proper operation in accordance with the spectrum usage rules for compliance with the European R&TTE directive 1999/5/EC. See the switch software guide for detailed instructions on use of this utility.

The Altitude 350-2 Access Point with integrated and detachable antennas are designed to be operated only indoors within all countries of the European Community. Some countries require limited channels of operation for indoor use. These restrictions are described in this section. For the most up to date restriction and limitations go to www.extremenetworks.com/go/rfcertification.htm.

NOTE

The Altitude 350-2 AP is completely configured and managed by the Summit WM series switch connected to the network Please follow the instructions in this software user guide to properly configure the Altitude 350-2 AP.

- The Altitude 350-2 wireless port requires the end user or installer to properly enter the correct country code into the switch software prior to operating the Altitude 350-2 AP, to allow for proper configuration in conformance with European National spectrum usage laws.
- After the first Altitude 350-2 wireless port is connected to the switch, each additional wireless port connected will inherit the operating configuration of the first Altitude 350-2 wireless port. The user or installer is responsible to ensure the first Altitude 350-2 wireless port is properly configured.
- The software within the switch will automatically limit the allowable channels and output power determined by the current country code entered. Incorrectly entering the country of operation or identifying the proper antenna used, may result in illegal operation and may cause harmful interference to other systems.
- This device employs a radar detection feature required for European Community operation in the 5 GHz band. This feature is automatically enabled when the country of operation is correctly configured for any European Community country. The presence of nearby radar operation may result in temporary interruption of operation of this device. The radar detection feature will automatically restart operation on a channel free of radar.
- The 5 GHz Turbo Mode feature is not enabled for use on the Altitude 350-2 AP Model 15938 and 15939.
- The AutoChannelSelect/SmartSelect setting of the 5 GHz described in the switch software guide must always remain enabled to ensure that automatic 5 GHz channel selection complies with European requirements. The current setting for this feature is found in the 5 GHz Radio Configuration Window as described in this switch software manual.
- The Altitude 350-2 AP with integral or detachable antennas may be used to transmit indoors and outdoors in countries of the European Community, as indicated in Table 24.
  Go to http://www.extremenetworks.com/go/rfcertification.htm for the most up to date limitation and restrictions.
- The Altitude 350-2 AP must be operated indoors only when using the 5150- 5350 MHz bands, channels 36, 40, 44, 48, 52, 56, 60, or 64. See Table 23 for permitted 5 GHz channels by country.
- The Altitude 350-2 AP with detachable antenna must be used only with antennas certified by Extreme Networks.
- The Altitude 350-2 AP may be operated indoors or outdoors in all countries of the European Community using the 2.4 GHz band: Channels 1 – 13, except where noted in Table 24.

- In Italy, the end user must apply for a license from the national spectrum authority to operate this device outdoors.
- In Belgium, outdoor operation is only permitted using the 2.46 - 2.4835 GHz band: Channel 13.
- In France, outdoor operation is only permitted using the 2.4 - 2.454 GHz band: Channels 1 - 7.

Permitted 5 GHz Channels for the European Community

Table 23 lists the 5 GHz channels approved for operation in the European Community.

Table 23: Permitted 5 GHz Channels in European Community Countries

Permitted Frequency Bands	Permitted Channel Numbers	Countries
5.15-5.25GHz	36, 40, 44, 48	Austria, Belgium
5.15-5.35GHz	36, 40, 44, 48, 52, 56, 60, 64	France, Switzerland, Liechtenstein
5.15-5.35* & 5.470-5.725GHz	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	Denmark, Finland, Germany, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, U.K.
5GHz Operation Not Allowed	None	Greece

European Spectrum Usage Rules

Table 24 lists the rules and restrictions for operating a 2.4 GHz or 5 GHz device in the European Community. Always use the latest software version for the most up-to-date channel list; some earlier software versions supply only a limited number of channels.

The Altitude 350-2 AP must be installed in the proper indoor or outdoor location. Use the installation utility provided with the switch software to insure proper set-up in accordance with all European spectrum usage rules.

Table 24: European Spectrum Usage Rules - Effective as of July 2005

Country	5.15-5.25 (GHz) Channels: 36,40,44,48	5.25-5.35 (GHz) Channels: 52,56,60,64	5.47-5.725 (GHz) Channels: 100,104,108,112,116,120,124,128,132,136,140	2.4-2.4835 (GHz) Channels: 1 to 13 (Except Where Noted)
Austria	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Belgium[a]	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor[a]
Bulgaria	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Denmark	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Cyprus	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Czech Rep.	Indoor Only	Indoor Only	Expect to Open Fall 2006	Indoor or Outdoor
Estonia	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Finland	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
France	Indoor Only	Indoor Only	Expect to Open Fall 2006	Indoor channels 1-13 **Outdoor channels 1-7 only**
Germany	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Greece	Indoor Only	Indoor Only	Indoor Only	Indoor Only

Table 24: European Spectrum Usage Rules - Effective as of July 2005 (Continued)

Country	5.15-5.25 (GHz) Channels: 36,40,44,48	5.25-5.35 (GHz) Channels: 52,56,60,64	5.47-5.725 (GHz) Channels: 100,104,108,112,116,120,124,128,132,136,140	2.4-2.4835 (GHz) Channels: 1 to 13 (Except Where Noted)
Hungary	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Iceland	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Ireland	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Italy	Indoor Only	Indoor Only	Indoor (Outdoor w/License)	Indoor (Outdoor w/License)
Latvia	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Liechtenstein	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Lithuania	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Luxembourg	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Netherlands	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Malta	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Norway	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Poland	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Portugal	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Slovak Rep.	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Slovenia	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Spain	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Sweden	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Switzerland	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
U. K.	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Turbo Mode	Not Allowed in 5GHz	Not Allowed in 5GHz	Not Allowed in 5GHz	Same 2.4 GHz rules as above
AdHoc Mode	Not Allowed	Not Allowed	Not Allowed	Same 2.4 GHz rules as above

[a] Belgium requires that the spectrum agency be notified if you deploy wireless links greater than 300 meters in outdoor public areas using 2.4 GHz band.

Declarations of Conformity

Table 25 presents the Extreme Networks declarations of conformity for the languages used in the European Community.

Table 25: Declaration of Conformity in Languages of the European Community

English	Hereby, Extreme Networks, declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Finnish	Valmistaja Extreme Networks vakuuttaa taten etta Radio LAN device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sita koskevien direktiivin muiden ehtojen mukainen.
Dutch	Hierbij verklaart Extreme Networks dat het toestel Radio LAN device in overeenstemming is met de essentiele eisen en de andere relevante bepalingen van richtlijn 1999/5/EG
	Bij deze verklaart Extreme Networks dat deze Radio LAN device voldoet aan de essentiele eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
French	Par la presente Extreme Networks declare que l'appareil Radio LAN device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE
	Par la presente, Extreme Networks declare que ce Radio LAN device est conforme aux exigences essentielles et aux autres dispositions de la directive 1999/5/CE qui lui sont applicables
Swedish	Harmed intygar Extreme Networks att denna Radio LAN device star I overensstammelse med de vasentliga egenskapskrav och ovriga relevanta bestammelser som framgar av direktiv 1999/5/EG.
Danish	Undertegnede Extreme Networks erklarer herved, at folgende udstyr Radio LAN device overholder de vasentlige krav og ovrige relevante krav i direktiv 1999/5/EF
German	Hiermit erklart Extreme Networks, dass sich diese Radio LAN device in Ubereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi)
	Hiermit erklart Extreme Networks die Ubereinstimmung des Gerates Radio LAN device mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
Greek	*ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Extreme Networks ΔΗΛΩΝΕΙ ΟΤΙ* Radio LAN device *ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ*
Italian	Con la presente Extreme Networks dichiara che questo Radio LAN device e conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Spanish	Por medio de la presente Extreme Networks declara que el Radio LAN device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE
Portuguese	Extreme Networks declara que este Radio LAN device esta conforme com os requisitos essenciais e outras disposicoes da Directiva 1999/5/CE.

Certifications of Other Countries

The Altitude 350-2 AP Model 15938 and 15939 has been certified for use in the countries listed in Table 26. When the Altitude 350-2 AP is connected to the Extreme Networks switch, the user is prompted to enter a country code. Once the correct country code is entered, the switch automatically sets up the Altitude 350-2 AP with the proper frequencies and power outputs for that country code.

Go to http://www.extremenetworks.com/go/rfcertification.htm for the most up to date list of certified countries.

NOTE

It is the responsibility of the end user to enter the proper country code for the country the device will be operated within.

Table 26: Other Country Specific Compliance Standards, Approvals and Declarations

Country	Standards, Approvals, Declarations	
Australia and New Zealand	• Altitude 350-2 AP (with Integrated or Detachable Antenna) • AS/NZS 4288 (Radio) • AS/NZX 3260 (Safety) • AS/NZS 3548 (Emissions) • EEE 802.11a/b/g • IEEE 802.3af (PoE)	ACN 090 029 066 • EN 300 328-2:2003-4 (2.4 GHz) • EN 301 893-1:2003-08 (5 GHz) • EN 301 489-17:2002-08 (RLAN) • EN 60950-1:2001 with Australia Deviation

Index

A

accounting
- setup on a WM-AD, 121

adding
- Altitude AP manually, 63

alarms
- overview of log types and levels, 220

allow all or approved APs
- for availability setup, 155

allow or deny in a filtering rule, 91

Altitude AP
- adding for availability setup, 155
- adding manually, 63
- assigning to a WM-AD, 107
- client disassociate, 203
- default configuration, 30, 35, 58, 66, 68, 79, 153, 155, 159
  - copy to defaults, 79
- international licensing, 56
- LED sequence in discovery, 58
- maintenance and reboot, 81
- radios, 56, 70
- static configuration, 75
- view statistics, 193

Analysis engine
- functions, 183

antennae on the Altitude AP, 56

authentication
- MAC-based, 119
- no RADIUS server, 87
- none on a WM-AD, 142
- on a WM-AD for AAA, 116
- on a WM-AD for Captive Portal, 109
- overview of types, 108
- protocols supported, 89, 112

Authentication, Authorization, Accounting (AAA)
- filter ID values (RADIUS policy), groups, 122
- set up 802.1x authentication, 116
- set up privacy on a WM-AD, 138

availability, 155

B

backup controller software configuration, 214

branch office, static configuration of
Altitude AP, 75

C

call data records (CDRs), 121

Captive Portal
- authentication on a WM-AD, 109
- configuring internal, external Captive Portal, 114
- defined, 89
- non-authenticated filtering rules, 126
- privacy mechanisms, 135
- set up a WM-AD topology, 98
- view sample page, 115

Check Point event logging, 167

configuring
- Captive Portal, internal, external, 114
- software - overview steps, 30
- static routes, 45

controller
- availability overview, 29
- back up software configuration, 214
- define management user names, passwords, 163
- define network time synchronization, 165
- defined as mobility manager for mobility, 159
- enable ELA event logging (Check Point), 167
- events during a failover, 158
- paired for availability, 153
- restore software configuration, 217
- set up third-party APs, 175
- system maintenance, 208
- system shutdown, 208

D

default filter, 131

default gateway on a WM-AD, 102

disassociate a wireless client, 203

discovery
- Altitude AP LED sequence, 58
- steps, 57

displays
- Altitude AP availability, 156, 193
- Altitude AP wired and wireless statistics, 193
- client location by foreign Summit switch, 163, 196
- client location by home, 163, 196
- list of displays, 191
- Summit switch tunnel traffic, 163, 196

documentation feedback, 10
Domain Name Server (DNS)
 in discovery, 57
DSCP classifications, 147
Dynamic Host Configuration Protocol (DHCP)
 for availability, 153
 for mobility (WM Access Domain Manager), 159
 Option 78 in discovery, 57
 relay on a WM-AD, 104
 required as part of solution, 22

E

event logging
 in Check Point, 167
 in Summit switch software, 220
exception filters
 on a WM-AD, 124
 port-based, 51
exclusions, IP address range on a WM-AD, 103

F

failover of a controller
 availability overview, 29
 events and recovery, 158
failover of a RADIUS server, 112
filtering
 default filter, 131
 exception filter on a WM-AD, 124
 filtering rules, overview of set up, 123
 for an AAA group, 133
 for Captive Portal authentication, 115
 non-authenticated filter for Captive Portal, 126
 non-authenticated filtering rules, examples, 128
 on a WM-AD for third-party APs, 177
 overview of packet filtering, 28
 overview, four types, 90
 port-based, 50
 rules for filter ID values, 129
 set filter ID values (RADIUS policy), 122
formatting conventions, 10
forwarding table report, 47

G

gateway, default, on a WM-AD, 102
global settings
 for a WM-AD, 92
 RADIUS servers for authentication, 111, 118, 120, 122
groups for Authentication, Authorization, Accounting (AAA), 122

H

health checking status of Altitude APs, 208
heartbeat messages, in WM Access Domain Manager feature, 159

I

IP address range on a WM-AD, 103

L

LED sequence
 in discovery, 58
login user name and password, 37
Login-LAT-Group, 129
 for WM-AD AAA authentication, 122
logs
 changing log level, 208
 event logging in Check Point, 167
 overview of types and levels, 220

M

MAC-based authentication, 119
Management Information Bases (MIBs) supported, 169
management port
 management traffic on data port, 45
 modify management port settings, 40
 port-based filtering, 50
management traffic
 enabling on a WM-AD, 100
mobility
 mobility manager and mobility agent, 159
 overview, 29
mobility manager
 defining a controller for mobility, 159
multicast
 for a WM-AD, 133

N

network assignment
 by AAA, 138
 by SSID for Captive Portal, 98
 options for a WM-AD, 87
 VLAN, 23, 26
network time synchronization, 165
next hop route for a WM-AD, 101
non-authenticated filter for Captive Portal, 115, 126

O

operating system software upgrade, 210
OSPF
    configuring, 47
    linkstate report, 50
    neighbor report, 50
    on a WM-AD, 101
overview, 28

P

password, for management users, 163
port
    port exception filters, 51
priority override, 144
privacy
    dynamic WEP on a WM-AD for AAA, 139
    encryption methods supported, 27
    on a WM-AD for AAA
        AAA, 138
    overview on a WM-AD, 92
    setup on a WM-AD for Captive Portal, 135
    static WEP for an AAA WM-AD, 138
    WPA v1 and WPA v2 on a WM-AD for AAA, 139
product key
    system maintenance, 210
protocols
    for authentication by Captive Portal, 112

Q

QoS (Quality of Service), 30, 88, 94, 142, 144, 238, 242
    admission control thresholds, 94
    advanced, 147
    modes, 144
    policy, 146

R

radio
    5 GHz (a) and 2.4 GHz (b/g), 56
    channels, 70, 74
radio settings
    view and modify, 70
RADIUS server
    deployment with no server, 87
    filter ID values, 129
    for authentication, 111, 118, 120, 122
    for MAC-based authentication, 119
    priority for redundancy, 112
    RADIUS accounting, 121
    RADIUS policy for a WM-AD, 122
    required as part of solution, 22
    VSAs in RADIUS message, 108
random delays, 59
read/write privileges, 163
reboot Altitude AP, 81
registration
    settings for availability setup, 155
reports
    AP inventory, 198
    forwarding table, 47, 198
    list of displays, 191
    OSPF linkstate, 50, 198
    OSPF neighbor, 50, 198
restore controller software configuration, 217
rogue detection, Summit spy feature, 184
routing
    configuring OSPF on data port, 47
    configuring static routes, 45
    next hop route on a WM-AD, 101
    overview, 28
routing table
    viewing, 47

S

scan results, Summit spy feature, 184
security of network, overview of methods, 26
service class, 142
Service Location Protocol (SLP)
    for availability, 153
    for mobility (WM Access Domain Manager), 159
    in discovery, 57
    required as part of solution, 22
    traffic allowed on data port, 45
    view slpdump tool report, 156
set up for a WM-AD, 175
shut down system, 208
Simple Network Management Protocol (SNMP)
    MIBs supported, 169
software
    maintenance of Altitude AP software, 81
    maintenance of Controller software, 210
SSID network assignment for Captive Portal, 98
static configuration of Altitude AP, 75
static routes
    configuring, 45
    viewing forwarding table report, 47
syslog event reporting
    define parameters, 208

T

third-party APs, 175
- defining a WM-AD for, 100
- in Summit spy feature, 188

topology of a WM-AD
- Captive Portal, 98

traces
- overview of log types and levels, 220

Type of Service (ToS/DSCP)
- on a WM-AD, 142
- Quality of Service, 30

U

user name and password for login, 37
user name and password, changing, 163

V

vendor specific attributes (VSA)
- in RADIUS message, 108
- RADIUS server
  - vendor specific attributes, 112, 119

VLAN
- configuration, 76, 97, 102, 144, 149, 150
- IDs, 150, 151

Voice-over-IP (VoIP)
- define multicast groups on a WM-AD, 133
- set up a WM-AD for, 142

vulnerable time interval, 59

W

Wi-Fi Multimedia (WMM)
- on a WM-AD, 142
- Quality of Service, 30

Wi-Fi Protected Access (WPA)
- overview on a WM-AD, 92
- PSK mode for Captive Portal, 136
- WPA v1 and v2 on a WM-AD for AAA, 139

Wired Equivalent Privacy (WEP)
- on a WM-AD for AAA, 138
- overview on a WM-AD, 92
- static for Captive Portal, 135

WM Access Domain Services (WM-AD), 28
- authentication by AAA (802.1x), 116
- authentication by Captive Portal, 109
- define filtering rules, 123
- defined, 85
- for third-party APs, 176
- global settings, 92
- multicast, 133
- network assignment overview, 87
- privacy for AAA, 138
- privacy overview, 135
- set up for VoIP, 142
- topology for Captive Portal, 98